REPRODUCING PERMISSION METHOD, RECORDING METHOD, AND RECORDING MEDIUM

Patent Number: JP10283270
Publication date: 1998-10-23
Inventor(s): YOSHIMOTO SHINICHI
Applicant(s):: FUJITSU LTD
Requested Patent: ☐ JP10283270
Application Number: JP19970091131 19970409
Priority Number(s):
IPC Classification: G06F12/14 ; G06F9/06 ; H04L9/32
EC Classification:
Equivalents:

Abstract

PROBLEM TO BE SOLVED: To provide a reproducing permission method which protects the copyright of information recorded in a recording medium without raising the production cost of the recording medium.
SOLUTION: Information (product constitution ID) peculiar to recording information (contents P) recorded in a recording medium 10 is used to encipher a first cipher key K to first encryption information (consent code L1), and the first cipher key is used to encipher recording information (contents P) to first encryption recording information (contents C), and peculiar information (product constitution ID) is recorded in a rewrite disable disable area on the recording medium 10, and first encryption information (consent code L1) and first encryption recording information (contents C) are recorded in the rewritable area on the recording medium 10; and at the time of reproducing, read-out peculiar information (product constitution ID) is used to decode first encryption information (consent code L1) to the first cipher key K, and the decoded first cipher key is used to decode first encryption recording information (contents C) to recording information (contents P).

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－283270

(43)公開日　平成10年(1998)10月23日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０６Ｆ	12/14	３２０	Ｇ０６Ｆ	12/14	３２０Ｆ
					３２０Ｂ
	9/06	５５０		9/06	５５０Ｚ
Ｈ０４Ｌ	9/32		Ｈ０４Ｌ	9/00	６７３Ｂ
					６７３Ｃ

審査請求　未請求　請求項の数21　ＯＬ　（全 23 頁）

(21)出願番号　特願平9－91131

(22)出願日　平成９年(1997)４月９日

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号

(72)発明者　吉本　真一
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

(74)代理人　弁理士　河野　登夫

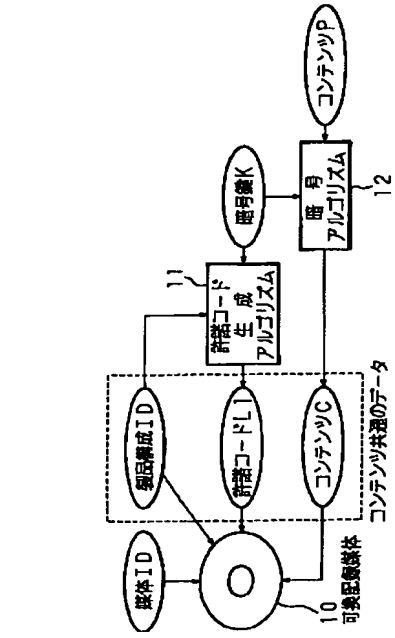
(54)【発明の名称】　再生許可方法、記録方法及び記録媒体

(57)【要約】

【課題】　記録媒体の製造コストの上昇を招くことなく、記録媒体に記録された情報の著作権を保護することができる再生許可方法の提供。

【解決手段】　記録媒体１０に記録される記録情報（コンテンツＰ）に固有の情報（製品構成ＩＤ）を用いて第１の暗号鍵（暗号鍵Ｋ）を第１の暗号化情報（許諾コードＬ１）に暗号化し、第１の暗号鍵を用いて記録情報（コンテンツＰ）を第１の暗号化記録情報（コンテンツＣ）に暗号化し、固有の情報（製品構成ＩＤ）を記録媒体１０上の書き換え不可能な領域に記録し、第１の暗号化情報（許諾コードＬ１）及び第１の暗号化記録情報（コンテンツＣ）を記録媒体１０上の書き換え可能な領域に記録し、再生時には、読み出した固有の情報（製品構成ＩＤ）を用いて第１の暗号化情報（許諾コードＬ１）を第１の暗号鍵（暗号鍵Ｋ）に復号化し、復号化した第１の暗号鍵を用いて第１の暗号化記録情報（コンテンツＣ）を記録情報（コンテンツＰ）に復号化する。

第１，２発明に係る再生許可方法、第１１発明に係る記録方法及び第１４，１５発明に係る記録媒体の実施の形態１を説明するための説明図



1

【特許請求の範囲】

【請求項１】　記録媒体に記録されている記録情報又は複製された該記録情報の再生を、前記記録媒体に記録されている所定の情報を用いて、許可する再生許可方法において、

前記記録されている記録情報に固有の情報を前記記録媒体に記録し、前記記録情報の再生に前記固有の情報を必要とすることを特徴とする再生許可方法。

【請求項２】　記録媒体に記録される記録情報に固有の情報を用いて所定の第１の暗号鍵を第１の暗号化情報に暗号化し、第１の暗号鍵を用いて前記記録情報を第１の暗号化記録情報に暗号化し、前記固有の情報は前記記録媒体上の書き換え不可能な領域に記録し、第１の暗号化情報及び第１の暗号化記録情報は前記記録媒体上の書き換え可能な領域に記録し、

再生時には、読み出した前記固有の情報を用いて第１の暗号化情報を第１の暗号鍵に復号化し、復号化した第１の暗号鍵を用いて第１の暗号化記録情報を前記記録情報に復号化することを特徴とする再生許可方法。

【請求項３】　所定の第１の情報を用いて、記録媒体に記録されている記録情報又は複製された該記録情報の再生を許可する再生許可方法において、

前記記録媒体用ドライブ装置に記録されているドライブ装置に固有の情報を、前記記録情報の再生に必要とすることを特徴とする再生許可方法。

【請求項４】　前記固有の情報を用いて第１の暗号鍵を第１の暗号化情報に暗号化し、第１の暗号鍵を用いて前記記録情報を第１の暗号化記録情報に暗号化し、第１の暗号化情報及び第１の暗号化記録情報は前記記録媒体上の書き換え可能な領域に記録し、

再生時には、前記固有の情報を用いて第１の暗号化情報を第１の暗号鍵に復号化し、復号化した第１の暗号鍵を用いて第１の暗号化記録情報を前記記録情報に復号化する請求項３記載の再生許可方法。

【請求項５】　前記固有の情報を用いて第１の暗号鍵を第１の暗号化情報に暗号化し、第１の暗号鍵を用いて前記記録情報を第１の暗号化記録情報に暗号化し、第１の暗号化情報及び第１の暗号化記録情報は前記記録媒体上の書き換え可能な領域に記録し、

最初の再生に先立って、前記固有の情報を用いて第１の暗号化情報を第１の暗号鍵に復号化し、復号化した第１の暗号鍵を、所定の第２の情報を用いて第２の暗号化情報に暗号化し、第２の暗号化情報を第１の暗号化情報に替えて前記記録媒体上の書き換え可能な領域に記録し、

再生時には、第２の情報を用いて第２の暗号化情報を第１の暗号鍵に復号化し、復号化した第１の暗号鍵を用いて第１の暗号化記録情報を前記記録情報に復号化する請求項３記載の再生許可方法。

【請求項６】　前記固有の情報を用いて第１の暗号鍵を第１の暗号化情報に暗号化し、第１の暗号鍵を用いて前記記録情報を第１の暗号化記録情報に暗号化し、第１の暗号化情報及び第１の暗号化記録情報は前記記録媒体上の書き換え可能な領域に記録し、

最初の再生に先立って、前記固有の情報を用いて第１の暗号化情報を第１の暗号鍵に復号化し、復号化した第１の暗号鍵を用いて第１の暗号化記録情報を前記記録情報に復号化し、復号化した前記記録情報を、第２の暗号鍵を用いて第２の暗号化記録情報に暗号化し、所定の第２の情報を用いて第２の暗号鍵を第３の暗号化情報に暗号化し、第３の暗号化情報を第１の暗号化情報に替えて、また、第２の暗号化記録情報を前記記録媒体上の書き換え可能な領域に記録し、

再生時には、第２の情報を用いて第３の暗号化情報を第２の暗号鍵に復号化し、復号化した第２の暗号鍵を用いて第２の暗号化記録情報を前記記録情報に復号化する請求項３記載の再生許可方法。

【請求項７】　前記固有の情報を第１の暗号鍵に暗号化し、第１の暗号鍵を用いて前記記録情報を第１の暗号化記録情報に暗号化し、第１の暗号化記録情報は前記記録媒体上の書き換え可能な領域に記録し、

最初の再生に先立って、前記固有の情報を第１の暗号鍵に暗号化し、第１の暗号鍵を用いて第１の暗号化記録情報を前記記録情報に復号化し、所定の第２の情報を第２の暗号鍵に暗号化し、復号化した前記記録情報を、第２の暗号鍵を用いて第２の暗号化記録情報に暗号化し、第２の暗号化記録情報を前記記録媒体上の書き換え可能な領域に記録し、

再生時には、第２の情報を第２の暗号鍵に暗号化し、第２の暗号鍵を用いて第２の暗号化記録情報を前記記録情報に復号化する請求項３記載の再生許可方法。

【請求項８】　第２の情報は、前記記録媒体から読み出した前記記録媒体毎に固有の情報である請求項５～７の何れかに記載の再生許可方法。

【請求項９】　第２の情報は、ユーザ毎に固有の情報である請求項５～７の何れかに記載の再生許可方法。

【請求項１０】　第２の情報は、前記ドライブ装置を制御するコンピュータに固有の情報である請求項５～７の何れかに記載の再生許可方法。

【請求項１１】　記録する記録情報に固有の情報を用いて所定の第１の暗号鍵を第１の暗号化情報に暗号化し、第１の暗号鍵を用いて前記記録情報を第１の暗号化記録情報に暗号化し、前記固有の情報を書き換え不可能な領域に記録し、第１の暗号化情報及び第１の暗号化記録情報を書き換え可能な領域に記録することを特徴とする記録媒体への記録方法。

【請求項１２】　ドライブ装置に記録されているドライブ装置に固有の情報を用いて第１の暗号鍵を第１の暗号化情報に暗号化し、記録する記録情報を第１の暗号鍵を用いて第１の暗号化記録情報に暗号化し、第１の暗号化情報及び第１の暗号化記録情報を書き換え可能な領域に

記録することを特徴とする記録媒体への記録方法。

【請求項１３】　ドライブ装置に記録されているドライブ装置に固有の情報を第１の暗号鍵に暗号化し、第１の暗号鍵を用いて、記録する記録情報を第１の暗号化記録情報に暗号化し、第１の暗号化記録情報を書き換え可能な領域に記録することを特徴とする記録媒体への記録方法。

【請求項１４】　請求項１に記載された再生許可方法に適用される記録媒体であって、

記録してある記録情報に固有の情報を記録してあることを特徴とする記録媒体。

【請求項１５】　前記固有の情報を用いて所定の暗号鍵から暗号化された暗号化情報を記録してある請求項１４記載の記録媒体。

【請求項１６】　請求項４に記載された再生許可方法に適用される記録媒体であって、

ドライブ装置に記録されているドライブ装置に固有の情報を用いて所定の暗号鍵から暗号化された暗号化情報を記録してあることを特徴とする記録媒体。

【請求項１７】　請求項２に記載された再生許可方法に適用される適用記録媒体に記録されている記録情報を再生する為のコンピュータプログラムを記録してある記録媒体であって、

読み出した、前記記録情報に固有の情報を用いて第１の暗号化情報を第１の暗号鍵に復号化するステップと、復号化した第１の暗号鍵を用いて第１の暗号化記録情報を前記記録情報に復号化するステップとを含むコンピュータプログラムを記録してあることを特徴とする記録媒体。

【請求項１８】　請求項４に記載された再生許可方法に適用される適用記録媒体に記録されている記録情報を再生する為のコンピュータプログラムを記録してある記録媒体であって、

前記適用記録媒体用ドライブ装置に記録されているドライブ装置に固有の情報を用いて第１の暗号化情報を第１の暗号鍵に復号化するステップと、復号化した第１の暗号鍵を用いて第１の暗号化記録情報を前記記録情報に復号化するステップとを含むコンピュータプログラムを記録してあることを特徴とする記録媒体。

【請求項１９】　請求項５に記載された再生許可方法に適用される適用記録媒体に記録されている記録情報を再生する為のコンピュータプログラムを記録してある記録媒体であって、

最初の再生に先立って、前記適用記録媒体用ドライブ装置に記録されているドライブ装置に固有の情報を用いて第１の暗号化情報を第１の暗号鍵に復号化するステップと、復号化した第１の暗号鍵を、所定の第２の情報を用いて第２の暗号化情報に暗号化するステップと、第２の暗号化情報を第１の暗号化情報に替えて前記適用記録媒体上の書き換え可能な領域に記録するステップと、

再生時には、第２の情報を用いて第２の暗号化情報を第１の暗号鍵に復号化するステップと、復号化した第１の暗号鍵を用いて第１の暗号化記録情報を前記記録情報に復号化するステップとを含むコンピュータプログラムを記録してあることを特徴とする記録媒体。

【請求項２０】　請求項６に記載された再生許可方法に適用される適用記録媒体に記録されている記録情報を再生する為のコンピュータプログラムを記録してある記録媒体であって、

最初の再生に先立って、前記適用記録媒体用ドライブ装置に記録されているドライブ装置に固有の情報を用いて第１の暗号化情報を第１の暗号鍵に復号化するステップと、復号化した第１の暗号鍵を用いて第１の暗号化記録情報を前記記録情報に復号化するステップと、復号化した前記記録情報を、第２の暗号鍵を用いて第２の暗号化記録情報に暗号化するステップと、所定の第２の情報を用いて第２の暗号鍵を第３の暗号化情報に暗号化するステップと、第３の暗号化情報を第１の暗号化情報に替えて、また、第２の暗号化記録情報を前記記録媒体上の書き換え可能な領域に記録するステップと、

再生時には、第２の情報を用いて第３の暗号化情報を第２の暗号鍵に復号化するステップと、復号化した第２の暗号鍵を用いて第２の暗号化記録情報を前記記録情報に復号化するステップとを含むコンピュータプログラムを記録してあることを特徴とする記録媒体。

【請求項２１】　請求項７に記載された再生許可方法に適用される適用記録媒体に記録されている記録情報を再生する為のコンピュータプログラムを記録してある記録媒体であって、

最初の再生に先立って、前記適用記録媒体用ドライブ装置に記録されているドライブ装置に固有の情報を第１の暗号鍵に暗号化するステップと、第１の暗号鍵を用いて第１の暗号化記録情報を前記記録情報に復号化するステップと、所定の第２の情報を第２の暗号鍵に暗号化するステップと、復号化した前記記録情報を、第２の暗号鍵を用いて第２の暗号化記録情報に暗号化するステップと、第２の暗号化記録情報を前記記録媒体上の書き換え可能な領域に記録するステップと、

再生時には、第２の情報を第２の暗号鍵に暗号化するステップと、第２の暗号鍵を用いて第２の暗号化記録情報を前記記録情報に復号化するステップとを含むコンピュータプログラムを記録してあることを特徴とする記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、著作権を保護する為に、ＤＶＤ（Digital Video Disc）、ＣＤ－ＲＯＭ及びＭＯ（Magneto-Optical）等の記録媒体に記録されている記録情報又は複製された記録情報の再生を許可する再生許可方法、その方法に適用される記録媒体への記録

方法、その方法に適用される記録媒体及びその方法の実施に直接使用されるコンピュータプログラムを記録してある記録媒体に関するものである。

【０００２】

【従来の技術】現在、記録媒体が備えている記録媒体毎に異なる固有の情報（媒体ＩＤ）を用いて、記録媒体に記録されているソフトウェア及びコンテンツ（記録情報、以下、コンテンツと記す）の著作権を保護する為の様々な再生許可方法が用いられている。図１６，１７は、従来の再生許可方法の一例を説明する為の説明図である。図１６は、記録媒体にコンテンツを記録するときの説明図であり、この再生許可方法では、まず、暗号アルゴリズムを備えたハードウェア又はソフトウェア７２を用いて、適当な暗号鍵Ｋによりコンテンツ Ｐを暗号化し、暗号化したコンテンツＣを記録媒体７０に記録する。

【０００３】次に、許諾コード生成アルゴリズムを備えたハードウェア又はソフトウェア７１を用いて、媒体ＩＤ及び暗号鍵Ｋから許諾コードＬ０を生成し、コンテンツＰの著作権所有者が保管する。ここでは、記録媒体７０の媒体ＩＤを暗号鍵として用いて、暗号鍵Ｋを暗号化し、許諾コードＬ０を生成してもよい。許諾コードＬ０は、コンテンツＰの著作権所有者が、コンテンツＰの使用を許可した者にのみ与えるものとする。

【０００４】図１７は、記録媒体７０のコンテンツＣを使用するときの説明図であり、コンテンツ使用者は、まず、コンテンツＰの著作権所有者から使用許可を受け、許諾コードＬ０を得ることが必要である。許諾コードＬ０を得ることができた場合、暗号鍵生成アルゴリズムを備えたハードウェア又はソフトウェア７３を用いて、媒体ＩＤ及び許諾コードＬ０から暗号鍵Ｋを得ることができる。媒体ＩＤを暗号鍵として用いて、許諾コードＬ０を復号し、暗号鍵Ｋを得てもよい。コンテンツ使用者は、暗号鍵Ｋを得ることにより、復号アルゴリズムを備えたハードウェア又はソフトウェア７４を用いて、暗号鍵Ｋ及び媒体ＩＤにより、暗号化されたコンテンツＣをコンテンツＰに復号して使用することが可能となる。

【０００５】この再生許可方法の特徴は、記録媒体７０毎に異なる媒体ＩＤを用いている為、コンテンツＰを使用するには、コンテンツＣが記録されている記録媒体７０毎に許諾コードＬ０を必要とするところにある。例えば、記録媒体Ａ用の許諾コードを持ったコンテンツ使用者が、コンテンツを記録媒体Ａから記録媒体Ｂに複写し、記録媒体Ｂに複写したコンテンツを使用しようとして、記録媒体Ａ用の許諾コードを用いたとしても、媒体ＩＤが異なるため、暗号鍵生成アルゴリズムを備えたハードウェア又はソフトウェア７３が正しい暗号鍵Ｋを生成することができず、コンテンツを正しく復号することができない。記録媒体Ｂに記録されたコンテンツを使用するには、記録媒体Ｂ用の許諾コードを必要とする。記録媒体Ａ用の許諾コードしか持たないコンテンツ使用者は、記録媒体Ａ上でのみコンテンツの使用を許可されるのである。

【０００６】さらに、この再生許可方法を応用すれば、以下のような方法が可能である。媒体ＩＤが付加された書き換えが可能な可換記録媒体（ＤＶＤ媒体、ＣＤ－ＲＯＭ媒体、ＭＯ媒体等）の書き換え可能な領域に暗号化されたコンテンツを記録し、書き換え不可能な領域に許諾コードを記録したものを作成する。コンテンツ使用者は、可換記録媒体に記録されたコンテンツの使用料金をコンテンツの著作権所有者に支払い、その可換記録媒体を受け取る。コンテンツ使用者は、既に可換記録媒体に記録されている許諾コードを用いて、その可換記録媒体上のコンテンツを自由に使用できるが、その可換記録媒体から他の可換記録媒体へそのコンテンツを複写した場合、許諾コードは複写されないので、他の可換記録媒体上のコンテンツを正しく復号することはできない。

【０００７】

【発明が解決しようとする課題】可換記録媒体は持ち運びが容易である為、上述した方法によりコンテンツ及び許諾コードが記録された可換記録媒体は、コンテンツ流通の手段として極めて有効である。しかし、この方法では、許諾コード及びコンテンツが記録された可換記録媒体を製造するのに大きなコストが掛かる問題がある。

【０００８】具体的には、可換記録媒体の製造工程において、媒体毎に変化する許諾コードを生成し、生成した許諾コードを対応する可換記録媒体に記録する等、一般的なＣＤ－ＲＯＭ等の製造設備より複雑な設備が必要となる。また、製造工程の後に行われる検査工程においても、可換記録媒体毎に許諾コードが異なるので、１枚ずつ可換記録媒体上の許諾コードが正しいか否かを検査しなければならず、その為、ＣＤ－ＲＯＭに較べて製造コストが高くなる。本発明は、前述したような事情に鑑みてなされたものであり、記録媒体の製造コストの上昇を招くことなく、記録媒体に記録された情報の著作権を保護することができる再生許可方法及び記録媒体を提供することを目的とする。

【０００９】

【課題を解決するための手段】第１発明に係る再生許可方法は、記録媒体に記録されている記録情報又は複製された該記録情報の再生を、前記記録媒体に記録されている所定の情報を用いて、許可する再生許可方法において、前記記録されている記録情報に固有の情報を前記記録媒体に記録し、前記記録情報の再生に前記固有の情報を必要とすることを特徴とする。

【００１０】この再生許可方法では、記録媒体に記録されている記録情報に固有の情報を記録媒体に記録し、記録情報の再生にその固有の情報を必要とするので、その固有の情報を読み出せた場合に限り、記録情報の再生を許可することができる。これにより、記録情報が同じで

ある記録媒体は、その他の内容構成も同一となるので、一括して製造、検査を行うことができ、製造コストの上昇を招くことなく、記録媒体に記録された情報の著作権を保護することができる。

【００１１】第２発明に係る再生許可方法は、記録媒体に記録される記録情報に固有の情報を用いて所定の第１の暗号鍵を第１の暗号化情報に暗号化し、第１の暗号鍵を用いて前記記録情報を第１の暗号化記録情報に暗号化し、前記固有の情報は前記記録媒体上の書き換え不可能な領域に記録し、第１の暗号化情報及び第１の暗号化記録情報は前記記録媒体上の書き換え可能な領域に記録し、再生時には、読み出した前記固有の情報を用いて第１の暗号化情報を第１の暗号鍵に復号化し、復号化した第１の暗号鍵を用いて第１の暗号化記録情報を前記記録情報に復号化することを特徴とする。

【００１２】この再生許可方法では、記録媒体に記録されている記録情報に固有の情報を用いて第１の暗号鍵を第１の暗号化情報に暗号化し、第１の暗号鍵を用いて記録情報を第１の暗号化記録情報に暗号化する。そして、記録情報に固有の情報は記録媒体上の書き換え不可能な領域に記録し、第１の暗号化情報及び第１の暗号化記録情報は記録媒体上の書き換え可能な領域に記録する。再生時には、読み出した記録情報に固有の情報を用いて第１の暗号化情報を第１の暗号鍵に復号化し、復号化した第１の暗号鍵を用いて第１の暗号化記録情報を記録情報に復号化する。

【００１３】これにより、別の記録媒体に複写した場合、記録情報に固有の情報は複写されないので、第１の暗号鍵が復号化できず、記録情報を再生できない。従って、記録媒体に記録されている記録情報の著作権を保護することができる。また、記録情報が同じである記録媒体は、その他の内容構成も同一となり、一括して製造、検査を行うことができるので、製造コストの上昇を招くことがない。

【００１４】第３発明に係る再生許可方法は、所定の第１の情報を用いて、記録媒体に記録されている記録情報又は複製された該記録情報の再生を許可する再生許可方法において、前記記録媒体用ドライブ装置に記録されているドライブ装置に固有の情報を、前記記録情報の再生に必要とすることを特徴とする。

【００１５】この再生許可方法では、記録媒体に記録されている記録情報の再生に、記録媒体用ドライブ装置に記録されているドライブ装置に固有の情報を必要とするので、ドライブ装置に固有の情報が異なるドライブ装置による再生は行えず、記録媒体に記録されている記録情報の著作権を保護することができる。また、同じドライブ装置に固有の情報による暗号化情報を記録される記録媒体は、その他の内容構成も略同一となり、一括して製造、検査を行うことができるので、製造コストの上昇を招くことがない。

【００１６】第４発明に係る再生許可方法は、前記固有の情報を用いて第１の暗号鍵を第１の暗号化情報に暗号化し、第１の暗号鍵を用いて前記記録情報を第１の暗号化記録情報に暗号化し、第１の暗号化情報及び第１の暗号化記録情報は前記記録媒体上の書き換え可能な領域に記録し、再生時には、前記固有の情報を用いて第１の暗号化情報を第１の暗号鍵に復号化し、復号化した第１の暗号鍵を用いて第１の暗号化記録情報を前記記録情報に復号化することを特徴とする。

【００１７】この再生許可方法では、ドライブ装置に固有の情報を用いて第１の暗号鍵を第１の暗号化情報に暗号化し、第１の暗号鍵を用いて記録情報を第１の暗号化記録情報に暗号化する。そして、第１の暗号化情報及び第１の暗号化記録情報は記録媒体上の書き換え可能な領域に記録する。再生時には、ドライブ装置に固有の情報を用いて第１の暗号化情報を第１の暗号鍵に復号化し、復号化した第１の暗号鍵を用いて第１の暗号化記録情報を記録情報に復号化する。

【００１８】これにより、ドライブ装置に固有の情報が異なるドライブ装置による再生は行えず、記録媒体に記録されている記録情報の著作権を保護することができる。また、同じドライブ装置に固有の情報による暗号化情報を記録される記録媒体は、その他の内容構成も略同一となり、一括して製造、検査を行うことができるので、製造コストの上昇を招くことがない。

【００１９】第５発明に係る再生許可方法は、前記固有の情報を用いて第１の暗号鍵を第１の暗号化情報に暗号化し、第１の暗号鍵を用いて前記記録情報を第１の暗号化記録情報に暗号化し、第１の暗号化情報及び第１の暗号化記録情報は前記記録媒体上の書き換え可能な領域に記録し、最初の再生に先立って、前記固有の情報を用いて第１の暗号化情報を第１の暗号鍵に復号化し、復号化した第１の暗号鍵を、所定の第２の情報を用いて第２の暗号化情報に暗号化し、第２の暗号化情報を第１の暗号化情報に替えて前記記録媒体上の書き換え可能な領域に記録し、再生時には、第２の情報を用いて第２の暗号化情報を第１の暗号鍵に復号化し、復号化した第１の暗号鍵を用いて第１の暗号化記録情報を前記記録情報に復号化することを特徴とする。

【００２０】この再生許可方法では、ドライブ装置に固有の情報を用いて第１の暗号鍵を第１の暗号化情報に暗号化し、第１の暗号鍵を用いて記録情報を第１の暗号化記録情報に暗号化する。そして、第１の暗号化情報及び第１の暗号化記録情報は記録媒体上の書き換え可能な領域に記録する。最初の再生に先立って、ドライブ装置に固有の情報を用いて第１の暗号化情報を第１の暗号鍵に復号化し、復号化した第１の暗号鍵を、所定の第２の情報を用いて第２の暗号化情報に暗号化する。そして、第２の暗号化情報を第１の暗号化情報に替えて記録媒体上の書き換え可能な領域に記録する。再生時には、第２の

情報を用いて第２の暗号化情報を第１の暗号鍵に復号化し、復号化した第１の暗号鍵を用いて第１の暗号化記録情報を記録情報に復号化する。

【００２１】これにより、最初の再生に先立つ暗号化情報の変更を、ドライブ装置に固有の情報が異なるドライブ装置では行えず、また、暗号化情報の変更後は、別の記録媒体に複写した場合に、第２の情報がなければ、記録情報に復号化することができないので、記録媒体に記録されている記録情報の著作権を保護することができる。また、同じドライブ装置に固有の情報による暗号化情報を記録される記録媒体は、その他の内容構成も略同一となり、一括して製造、検査を行うことができるので、製造コストの上昇を招くことがない。

【００２２】第６発明に係る再生許可方法は、前記固有の情報を用いて第１の暗号鍵を第１の暗号化情報に暗号化し、第１の暗号鍵を用いて前記記録情報を第１の暗号化記録情報に暗号化し、第１の暗号化情報及び第１の暗号化記録情報は前記記録媒体上の書き換え可能な領域に記録し、最初の再生に先立って、前記固有の情報を用いて第１の暗号化情報を第１の暗号鍵に復号化し、復号化した第１の暗号鍵を用いて第１の暗号化記録情報を前記記録情報に復号化し、復号化した前記記録情報を、第２の暗号鍵を用いて第２の暗号化記録情報に暗号化し、第２の情報を用いて第２の暗号鍵を第３の暗号化情報に暗号化し、第３の暗号化情報を第１の暗号化情報に替えて、また、第２の暗号化記録情報を前記記録媒体上の書き換え可能な領域に記録し、再生時には、第２の情報を用いて第３の暗号化情報を第２の暗号鍵に復号化し、復号化した第２の暗号鍵を用いて第２の暗号化記録情報を前記記録情報に復号化することを特徴とする。

【００２３】この再生許可方法では、ドライブ装置に固有の情報を用いて第１の暗号鍵を第１の暗号化情報に暗号化し、第１の暗号鍵を用いて記録情報を第１の暗号化記録情報に暗号化する。そして、第１の暗号化情報及び第１の暗号化記録情報は記録媒体上の書き換え可能な領域に記録する。

【００２４】最初の再生に先立って、ドライブ装置に固有の情報を用いて第１の暗号化情報を第１の暗号鍵に復号化し、復号化した第１の暗号鍵を用いて第１の暗号化記録情報を記録情報に復号化する。復号化した記録情報は、第２の暗号鍵を用いて第２の暗号化記録情報に暗号化し、第２の情報を用いて第２の暗号鍵を第３の暗号化情報に暗号化する。そして、第３の暗号化情報を第１の暗号化情報に替えて、また、第２の暗号化記録情報を記録媒体上の書き換え可能な領域に記録する。再生時には、第２の情報を用いて第３の暗号化情報を第２の暗号鍵に復号化し、復号化した第２の暗号鍵を用いて第２の暗号化記録情報を記録情報に復号化する。

【００２５】これにより、最初の再生に先立つ暗号化情報及び暗号化記録情報の変更を、ドライブ装置に固有の情報が異なるドライブ装置では行えず、また、暗号化情報及び暗号化記録情報の変更後は、別の記録媒体に複写した場合に、第２の情報がなければ、記録情報に復号化することができないので、記録媒体に記録されている記録情報の著作権を保護することができる。また、同じドライブ装置に固有の情報による暗号化情報を記録される記録媒体は、その他の内容構成も略同一となり、一括して製造、検査を行うことができるので、製造コストの上昇を招くことがない。

【００２６】第７発明に係る再生許可方法は、前記固有の情報を第１の暗号鍵に暗号化し、第１の暗号鍵を用いて前記記録情報を第１の暗号化記録情報に暗号化し、第１の暗号化記録情報は前記記録媒体上の書き換え可能な領域に記録し、最初の再生に先立って、前記固有の情報を第１の暗号鍵に暗号化し、第１の暗号鍵を用いて第１の暗号化記録情報を前記記録情報に復号化し、第２の情報を第２の暗号鍵に暗号化し、復号化した前記記録情報を、第２の暗号鍵を用いて第２の暗号化記録情報に暗号化し、第２の暗号化記録情報を前記記録媒体上の書き換え可能な領域に記録し、再生時には、第２の情報を第２の暗号鍵に暗号化し、第２の暗号鍵を用いて第２の暗号化記録情報を前記記録情報に復号化することを特徴とする。

【００２７】この再生許可方法では、ドライブ装置に固有の情報を第１の暗号鍵に暗号化し、第１の暗号鍵を用いて記録情報を第１の暗号化記録情報に暗号化する。そして、第１の暗号化記録情報は記録媒体上の書き換え可能な領域に記録する。最初の再生に先立って、ドライブ装置に固有の情報を第１の暗号鍵に暗号化し、第１の暗号鍵を用いて第１の暗号化記録情報を記録情報に復号化する。そして、第２の情報を第２の暗号鍵に暗号化し、復号化した記録情報を、第２の暗号鍵を用いて第２の暗号化記録情報に暗号化し、第２の暗号化記録情報を記録媒体上の書き換え可能な領域に記録する。再生時には、第２の情報を第２の暗号鍵に暗号化し、第２の暗号鍵を用いて第２の暗号化記録情報を記録情報に復号化する。

【００２８】これにより、最初の再生に先立つ暗号化記録情報の変更を、ドライブ装置に固有の情報が異なるドライブ装置では行えず、また、暗号化記録情報の変更後は、別の記録媒体に複写した場合に、第２の情報がなければ、記録情報に復号化することができないので、記録媒体に記録されている記録情報の著作権を保護することができる。また、同じドライブ装置に固有の情報による暗号鍵により暗号化された暗号化記録情報を記録される記録媒体は、その他の内容構成も略同一となり、一括して製造、検査を行うことができるので、製造コストの上昇を招くことがない。

【００２９】第８発明に係る再生許可方法は、第２の情報は、前記記録媒体から読み出した前記記録媒体毎に固有の情報であることを特徴とする。

【００３０】この再生許可方法では、第２の情報は、記録媒体から読み出した記録媒体毎に固有の情報であるので、最初の再生に先立つ暗号化情報又は暗号化記録情報の変更後は、別の記録媒体に複写した場合に、記録媒体毎に固有の情報は複写されず、記録情報に復号化することができないので、記録媒体に記録されている記録情報の著作権を保護することができる。

【００３１】第９発明に係る再生許可方法は、第２の情報は、ユーザ毎に固有の情報であることを特徴とする。

【００３２】この再生許可方法では、第２の情報は、ユーザ毎に固有の情報であるので、最初の再生に先立つ暗号化情報又は暗号化記録情報の変更後は、別の記録媒体に複写した場合に、ユーザが異なれば、記録情報に復号化することができないので、記録媒体に記録されている記録情報の著作権を保護することができる。

【００３３】第１０発明に係る再生許可方法は、第２の情報は、前記ドライブ装置を制御するコンピュータに固有の情報であることを特徴とする。

【００３４】この再生許可方法では、第２の情報は、ドライブ装置を制御するコンピュータに固有の情報であるので、最初の再生に先立つ暗号化情報又は暗号化記録情報の変更後は、別の記録媒体に複写した場合に、ドライブ装置を制御するコンピュータが異なれば、記録情報に復号化することができないので、記録媒体に記録されている記録情報の著作権を保護することができる。

【００３５】第１１発明に係る記録方法は、記録する記録情報に固有の情報を用いて所定の第１の暗号鍵を第１の暗号化情報に暗号化し、第１の暗号鍵を用いて前記記録情報を第１の暗号化記録情報に暗号化し、前記固有の情報を書き換え不可能な領域に記録し、第１の暗号化情報及び第１の暗号化記録情報を書き換え可能な領域に記録することを特徴とする。

【００３６】この記録方法では、記録媒体に記録する記録情報に固有の情報を用いて第１の暗号鍵を第１の暗号化情報に暗号化し、第１の暗号鍵を用いて記録情報を第１の暗号化記録情報に暗号化する。そして、記録情報に固有の情報は記録媒体上の書き換え不可能な領域に記録し、第１の暗号化情報及び第１の暗号化記録情報は記録媒体上の書き換え可能な領域に記録する。これにより、別の記録媒体に複写した場合、記録情報に固有の情報は複写されないので、第１の暗号鍵が復号化できず、記録情報を再生できない。従って、記録媒体に記録されている記録情報の著作権を保護することができる。また、記録情報が同じである記録媒体は、その他の内容構成も同一となり、一括して製造、検査を行うことができるので、製造コストの上昇を招くことがない。

【００３７】第１２発明に係る記録方法は、ドライブ装置に記録されているドライブ装置に固有の情報を用いて第１の暗号鍵を第１の暗号化情報に暗号化し、記録する記録情報を第１の暗号鍵を用いて第１の暗号化記録情報に暗号化し、第１の暗号化情報及び第１の暗号化記録情報を書き換え可能な領域に記録することを特徴とする。

【００３８】この記録方法では、ドライブ装置に固有の情報を用いて第１の暗号鍵を第１の暗号化情報に暗号化し、第１の暗号鍵を用いて記録情報を第１の暗号化記録情報に暗号化する。そして、第１の暗号化情報及び第１の暗号化記録情報は記録媒体上の書き換え可能な領域に記録する。これにより、ドライブ装置に固有の情報が異なるドライブ装置による再生は行えず、記録媒体に記録されている記録情報の著作権を保護することができる。また、ドライブ装置に固有の同じ情報による暗号化情報を記録される記録媒体は、その他の内容構成も略同一となり、一括して製造、検査を行うことができるので、製造コストの上昇を招くことがない。

【００３９】第１３発明に係る記録方法は、ドライブ装置に記録されているドライブ装置に固有の情報を第１の暗号鍵に暗号化し、第１の暗号鍵を用いて、記録する記録情報を第１の暗号化記録情報に暗号化し、第１の暗号化記録情報を書き換え可能な領域に記録することを特徴とする。

【００４０】この記録方法では、ドライブ装置に固有の情報を第１の暗号鍵に暗号化し、第１の暗号鍵を用いて記録情報を第１の暗号化記録情報に暗号化する。そして、第１の暗号化記録情報を記録媒体上の書き換え可能な領域に記録する。これにより、最初の再生に先立つ暗号化記録情報の変更を、ドライブ装置に固有の情報が異なるドライブ装置では行えないので、記録媒体に記録されている記録情報の著作権を保護することができる。また、同じドライブ装置に固有の情報による暗号鍵により暗号化された暗号化記録情報を記録される記録媒体は、その他の内容構成も略同一となり、一括して製造、検査を行うことができるので、製造コストの上昇を招くことがない。

【００４１】第１４発明に係る記録媒体は、請求項１に記載された再生許可方法に適用される記録媒体であって、記録してある記録情報に固有の情報を記録してあることを特徴とする。

【００４２】この記録媒体では、記録情報に固有の情報を記録媒体に記録し、記録情報の再生にその固有の情報を必要としてあるので、その固有の情報を読み出せた場合に限り、記録情報の再生を許可することができる。これにより、記録情報が同じである場合は、その他の内容構成も同一となるので、一括して製造、検査を行うことができ、製造コストの上昇を招くことなく、記録された情報の著作権を保護することができる。

【００４３】第１５発明に係る記録媒体は、前記固有の情報を用いて所定の暗号鍵から暗号化された暗号化情報を記録してあることを特徴とする。

【００４４】この記録媒体では、記録情報に固有の情報を用いて所定の暗号鍵から暗号化された暗号化情報を記

録しており、複写されても記録情報に固有の情報は複写されず、暗号化情報を暗号鍵に復号できないので、記録情報が同じであれば、その他の内容構成も同一となり、一括して製造、検査を行うことができ、製造コストの上昇を招くことなく、記録された情報の著作権を保護することができる。

【００４５】第１６発明に係る記録媒体は、請求項４に記載された再生許可方法に適用される記録媒体であって、ドライブ装置に記録されているドライブ装置に固有の情報を用いて所定の暗号鍵から暗号化された暗号化情報を記録してあることを特徴とする。

【００４６】この記録媒体では、第１の暗号化情報及び第１の暗号化記録情報は書き換え可能な領域に記録しているので、再生時には、ドライブ装置に固有の情報を用いて第１の暗号化情報を第１の暗号鍵に復号化でき、復号化した第１の暗号鍵を用いて第１の暗号化記録情報を記録情報に復号化できる。これにより、ドライブ装置に固有の情報が異なるドライブ装置による再生は行えず、記録されている記録情報の著作権を保護することができる。また、同じドライブ装置に固有の情報による暗号化情報を記録される記録媒体は、その他の内容構成も略同一となり、一括して製造、検査を行うことができるので、製造コストの上昇を招くことがない。

【００４７】第１７発明に係る記録媒体は、請求項２に記載された再生許可方法に適用される適用記録媒体に記録されている記録情報を再生する為のコンピュータプログラムを記録してある記録媒体であって、読み出した、前記記録情報に固有の情報を用いて第１の暗号化情報を第１の暗号鍵に復号化するステップと、復号化した第１の暗号鍵を用いて第１の暗号化記録情報を前記記録情報に復号化するステップとを含むコンピュータプログラムを記録してあることを特徴とする。

【００４８】この記録媒体に記録してあるコンピュータプログラムにより制御されるコンピュータでは、適用記録媒体に記録されている記録情報を再生するときに、読み出した記録情報に固有の情報を用いて第１の暗号化情報を第１の暗号鍵に復号化し、復号化した第１の暗号鍵を用いて第１の暗号化記録情報を記録情報に復号化する。これにより、別の記録媒体に複写した場合、記録情報に固有の情報は複写されないので、第１の暗号鍵が復号化できず、記録情報を再生できない。従って、記録媒体に記録されている記録情報の著作権を保護することができる。

【００４９】第１８発明に係る記録媒体は、請求項４に記載された再生許可方法に適用される適用記録媒体に記録されている記録情報を再生する為のコンピュータプログラムを記録してある記録媒体であって、前記適用記録媒体用ドライブ装置に記録されているドライブ装置に固有の情報を用いて第１の暗号化情報を第１の暗号鍵に復号化するステップと、復号化した第１の暗号鍵を用いて第１の暗号化記録情報を前記記録情報に復号化するステップとを含むコンピュータプログラムを記録してあることを特徴とする。

【００５０】この記録媒体に記録してあるコンピュータプログラムにより制御されるコンピュータでは、適用記録媒体に記録されている記録情報を再生するときに、ドライブ装置に固有の情報を用いて第１の暗号化情報を第１の暗号鍵に復号化し、復号化した第１の暗号鍵を用いて第１の暗号化記録情報を記録情報に復号化する。これにより、ドライブ装置に固有の情報が異なるドライブ装置による再生は行えず、記録媒体に記録されている記録情報の著作権を保護することができる。

【００５１】第１９発明に係る記録媒体は、請求項５に記載された再生許可方法に適用される適用記録媒体に記録されている記録情報を再生する為のコンピュータプログラムを記録してある記録媒体であって、最初の再生に先立って、前記適用記録媒体用ドライブ装置に記録されているドライブ装置に固有の情報を用いて第１の暗号化情報を第１の暗号鍵に復号化するステップと、復号化した第１の暗号鍵を、所定の第２の情報を用いて第２の暗号化情報に暗号化するステップと、第２の暗号化情報を第１の暗号化情報に替えて前記適用記録媒体上の書き換え可能な領域に記録するステップと、再生時には、第２の情報を用いて第２の暗号化情報を第１の暗号鍵に復号化するステップと、復号化した第１の暗号鍵を用いて第１の暗号化記録情報を前記記録情報に復号化するステップとを含むコンピュータプログラムを記録してあることを特徴とする。

【００５２】この記録媒体に記録してあるコンピュータプログラムにより制御されるコンピュータでは、適用記録媒体に記録されている記録情報の最初の再生に先立って、ドライブ装置に固有の情報を用いて第１の暗号化情報を第１の暗号鍵に復号化し、復号化した第１の暗号鍵を、所定の第２の情報を用いて第２の暗号化情報に暗号化する。そして、第２の暗号化情報を第１の暗号化情報に替えて記録媒体上の書き換え可能な領域に記録する。記録情報の再生時には、第２の情報を用いて第２の暗号化情報を第１の暗号鍵に復号化し、復号化した第１の暗号鍵を用いて第１の暗号化記録情報を記録情報に復号化する。

【００５３】これにより、最初の再生に先立つ暗号化情報の変更を、ドライブ装置に固有の情報が異なるドライブ装置では行えず、また、暗号化情報の変更後は、別の記録媒体に複写した場合に、第２の情報がなければ、記録情報に復号化することができないので、記録媒体に記録されている記録情報の著作権を保護することができる。

【００５４】第２０発明に係る記録媒体は、請求項６に記載された再生許可方法に適用される適用記録媒体に記録されている記録情報を再生する為のコンピュータプロ

グラムを記録してある記録媒体であって、最初の再生に先立って、前記適用記録媒体用ドライブ装置に記録されているドライブ装置に固有の情報を用いて第１の暗号化情報を第１の暗号鍵に復号化するステップと、復号化した第１の暗号鍵を用いて第１の暗号化記録情報を前記記録情報に復号化するステップと、復号化した前記記録情報を、第２の暗号鍵を用いて第２の暗号化記録情報に暗号化するステップと、所定の第２の情報を用いて第２の暗号鍵を第３の暗号化情報に暗号化するステップと、第３の暗号化情報を第１の暗号化情報に替えて、また、第２の暗号化記録情報を前記記録媒体上の書き換え可能な領域に記録するステップと、再生時には、第２の情報を用いて第３の暗号化情報を第２の暗号鍵に復号化するステップと、復号化した第２の暗号鍵を用いて第２の暗号化記録情報を前記記録情報に復号化するステップとを含むコンピュータプログラムを記録してあることを特徴とする。

【００５５】この記録媒体に記録してあるコンピュータプログラムにより制御されるコンピュータでは、適用記録媒体に記録されている記録情報の最初の再生に先立って、ドライブ装置に固有の情報を用いて第１の暗号化情報を第１の暗号鍵に復号化し、復号化した第１の暗号鍵を用いて第１の暗号化記録情報を記録情報に復号化する。復号化した記録情報は、第２の暗号鍵を用いて第２の暗号化記録情報に暗号化し、第２の情報を用いて第２の暗号鍵を第３の暗号化情報に暗号化する。そして、第３の暗号化情報を第１の暗号化情報に替えて、また、第２の暗号化記録情報を記録媒体上の書き換え可能な領域に記録する。記録情報の再生時には、第２の情報を用いて第３の暗号化情報を第２の暗号鍵に復号化し、復号化した第２の暗号鍵を用いて第２の暗号化記録情報を記録情報に復号化する。

【００５６】これにより、最初の再生に先立つ暗号化情報及び暗号化記録情報の変更を、ドライブ装置に固有の情報が異なるドライブ装置では行えず、また、暗号化情報及び暗号化記録情報の変更後は、別の記録媒体に複写した場合に、第２の情報がなければ、記録情報に復号化することができないので、記録媒体に記録されている記録情報の著作権を保護することができる。

【００５７】第２１発明に係る記録媒体は、請求項７に記載された再生許可方法に適用される適用記録媒体に記録されている記録情報を再生する為のコンピュータプログラムを記録してある記録媒体であって、最初の再生に先立って、前記適用記録媒体用ドライブ装置に記録されているドライブ装置に固有の情報を第１の暗号鍵に暗号化するステップと、第１の暗号鍵を用いて第１の暗号化記録情報を前記記録情報に復号化するステップと、所定の第２の情報を第２の暗号鍵に暗号化するステップと、復号化した前記記録情報を、第２の暗号鍵を用いて第２の暗号化記録情報に暗号化するステップと、第２の暗号化記録情報を前記記録媒体上の書き換え可能な領域に記録するステップと、再生時には、第２の情報を第２の暗号鍵に暗号化するステップと、第２の暗号鍵を用いて第２の暗号化記録情報を前記記録情報に復号化するステップとを含むコンピュータプログラムを記録してあることを特徴とする。

【００５８】この記録媒体に記録してあるコンピュータプログラムにより制御されるコンピュータでは、適用記録媒体に記録されている記録情報の最初の再生に先立って、ドライブ装置に固有の情報を第１の暗号鍵に暗号化し、第１の暗号鍵を用いて第１の暗号化記録情報を記録情報に復号化する。そして、第２の情報を第２の暗号鍵に暗号化し、復号化した記録情報を、第２の暗号鍵を用いて第２の暗号化記録情報に暗号化し、第２の暗号化記録情報を記録媒体上の書き換え可能な領域に記録する。記録情報の再生時には、第２の情報を第２の暗号鍵に暗号化し、第２の暗号鍵を用いて第２の暗号化記録情報を記録情報に復号化する。

【００５９】これにより、最初の再生に先立つ暗号化記録情報の変更を、ドライブ装置に固有の情報が異なるドライブ装置では行えず、また、暗号化記録情報の変更後は、別の記録媒体に複写した場合に、第２の情報がなければ、記録情報に復号化することができないので、記録媒体に記録されている記録情報の著作権を保護することができる。

【００６０】

【発明の実施の形態】以下に、本発明をその実施の形態を示す図面に基づいて説明する。

実施の形態１．図１は、第１，２発明に係る再生許可方法、第１１発明に係る記録方法及び第１４，１５発明に係る記録媒体の実施の形態１を説明する為の説明図であり、書き換えが可能な可換記録媒体に記録する情報の生成方法を説明する為の説明図である。この生成方法は、可換記録媒体１０（記録媒体）に記録するコンテンツ構成及び種類に対応する製品構成ＩＤ（記録情報に固有の情報）と、コンテンツＰ（記録情報）用の暗号鍵Ｋ（第１の暗号鍵）とから許諾コード生成アルゴリズムを備えたハードウェア又はソフトウェア１１により、許諾コードＬ１（第１の暗号化情報）を生成する。製品構成ＩＤ及び可換記録媒体毎の媒体ＩＤは、可換記録媒体１０の書き換えが不可能な領域に記録する。

【００６１】コンテンツＰ用の暗号鍵Ｋから暗号アルゴリズムを備えたハードウェア又はソフトウェア１２により、コンテンツＰを暗号化してコンテンツＣ（第１の暗号化記録情報）を生成し、前述した許諾コードＬ１と共に、可換記録媒体１０の書き換えが可能な領域に記録する。

【００６２】従来の再生許可方法（図１６）では、媒体ＩＤに依存した許諾コードＬ０を生成していたが、媒体ＩＤ毎に許諾コードＬ０を生成しなければならないの

で、製造設備が複雑になり、製造コストの上昇を招いていた。一方、図１に示した再生許可方法では、製品構成ＩＤ毎に許諾コードＬ１とコンテンツＣとが共通のデータとなり、従来の再生許可方法（図１６）より製造設備が簡単になり、製造コストを低く押さえることが可能となる。

【００６３】図２は、可換記録媒体１０に記録されたコンテンツＣの利用方法を説明する為の説明図である。この利用方法では、可換記録媒体１０から製品構成ＩＤ及び許諾コードＬ１を読出し、暗号アルゴリズムを備えたハードウェア又はソフトウェア１３を用いて、製品構成ＩＤ及び許諾コードＬ１から暗号鍵Ｋを得る。次に、得られた暗号鍵Ｋにより、復号アルゴリズムを備えたハードウェア又はソフトウェア１４を用いて、暗号化されたコンテンツＣをコンテンツＰに復号する。これにより、コンテンツＰを使用することが可能となる。

【００６４】図３は、第１，２発明に係る再生許可方法に使用する可換記録媒体の製造工程を説明する為の説明図である。この製造工程では、まず、製造計画を立てる。製造計画では、可換記録媒体に記録するコンテンツの種類及び構成を決定し、このコンテンツの種類及び構成に対応する製品構成ＩＤを決定して、コンテンツの種類及び構成と製品構成ＩＤとの対応関係をメインコンピュータ８０のデータベースに登録する。次いで、メインコンピュータ８０により製造計画表を作成する。製造計画表には、製品構成ＩＤ、最初に製造される可換記録媒体の開始媒体ＩＤ及び製造枚数が記録されている。

【００６５】製造開始に当たって、メインコンピュータ８０は、製造計画表に従って、製造すべき可換記録媒体の製品構成ＩＤと製造枚数を得、データベースサーバ８１及びＩＤ記録機８５に可換記録媒体製造の指示を出す。ＩＤ記録機８５は、メインコンピュータ８０から製造枚数、開始媒体ＩＤ及び製品構成ＩＤを受け取り、開始媒体ＩＤを媒体ＩＤカウンタの初期値として設定する。次に、ＩＤ記録機８５は、ＩＤが記録されていない可換記録媒体８４の書き換えが不可能な領域に、媒体ＩＤカウンタが指示する媒体ＩＤと製品構成ＩＤとを記録する。媒体ＩＤカウンタは、可換記録媒体８４に媒体ＩＤが記録される都度インクリメントされる。これにより、媒体ＩＤと製品構成ＩＤとが記録された可換記録媒体８６を得ることができる。

【００６６】一方、データベースサーバ８１では、上述した方法（図１）により、コンテンツの暗号鍵を生成し、生成した暗号鍵を用いてコンテンツ群を暗号化する。このとき、暗号鍵と製品構成ＩＤとの対応関係をデータベースに保存する。次に、製品構成ＩＤに依存する許諾コードを生成する。これにより、可換記録媒体８６に記録する全データ（暗号化されたコンテンツ群及び許諾コード）が決定され、この全データは複写機８２に与えられる。複写機８２では、暗号化されたコンテンツ群及び許諾コードを、製造すべき枚数分の可換記録媒体８６の書き換えが可能な領域に複写し、製品である可換記録媒体８３を製造する。

【００６７】実施の形態２．図４は、第３～５，８～１０発明に係る再生許可方法、第１２発明に係る記録方法及び第１６発明に係る記録媒体の実施の形態２を説明する為の説明図であり、書き換えが可能な可換記録媒体に記録する情報の生成方法を説明する為の説明図である。この生成方法は、可換記録媒体用ドライブ装置メーカ２１によって決められ、可換記録媒体用ドライブ装置に記録されているドライブＩＤ（ドライブ装置に固有の情報）と、コンテンツＰ（記録情報）用の暗号鍵Ｋ（第１の暗号鍵）とから許諾コード生成アルゴリズムを備えたハードウェア又はソフトウェア２２により、許諾コードＬ１（第１の暗号化情報）を生成する。

【００６８】コンテンツＰ用の暗号鍵Ｋから暗号アルゴリズムを備えたハードウェア又はソフトウェア２３により、コンテンツＰを暗号化してコンテンツＣ（第１の暗号化記録情報）を生成し、前述した許諾コードＬ１と共に、可換記録媒体２０の書き換えが可能な領域に記録する。可換記録媒体毎の媒体ＩＤ（第２の情報、記録媒体毎に固有の情報）は、可換記録媒体２０の書き換えが不可能な領域に記録する。

【００６９】従来の再生許可方法（図１６）では、媒体ＩＤに依存した許諾コードＬ０を生成していたが、媒体ＩＤ毎に許諾コードＬ０を生成しなければならないので、製造設備が複雑になり、製造コストの上昇を招いていた。一方、図１に示した再生許可方法では、ドライブＩＤ毎に許諾コードＬ１とコンテンツＣとが共通のデータとなり、従来の再生許可方法（図１６）より製造設備が簡単になり、製造コストを低く押さえることが可能となる。

【００７０】図５は、可換記録媒体２０に記録されたコンテンツが初めて利用される前に行われる許諾コードの変更方法を説明する為の説明図である。コンテンツ使用者が可換記録媒体２０に記録されたコンテンツＣを利用するとき、可換記録媒体用ドライブ装置２４は、まず、可換記録媒体２０に記録されているコンテンツ利用情報を参照し、コンテンツが既に利用されているか否かを検査する。コンテンツが利用されていないときは、ドライブＩＤに依存する許諾コードＬ１を、媒体ＩＤに依存する許諾コードＬ２（第２の暗号化情報）に変更する。

【００７１】許諾コードＬ１から許諾コードＬ２への変更は以下のように行われる。可換記録媒体用ドライブ装置２４から得られたドライブＩＤと、可換記録媒体２０から読み出された許諾コードＬ１とから、暗号鍵生成アルゴリズムを備えたハードウェア又はソフトウェア２５を用いて、暗号鍵Ｋを一時的に生成する。これにより、ドライブＩＤが異なる可換記録媒体用ドライブ装置では、暗号鍵Ｋを生成することができず、許諾コードの変

更を行うことはできない。次に、許諾コード生成アルゴリズムを備えたハードウェア又はソフトウェア２６を用いて、可換記録媒体２０から読み出した媒体ＩＤと暗号鍵Ｋとから、許諾コードＬ２を生成する。次に、得られた許諾コードＬ２を可換記録媒体２０の書き換えが可能な領域に記録する。

【００７２】許諾コードＬ２を可換記録媒体２０に記録した後、可換記録媒体２０上のコンテンツ利用情報を「コンテンツは既に利用された」の意味に変更する。これにより、以後、コンテンツ利用情報を参照することによって、「コンテンツは既に利用された」と判断され、許諾コードＬ２の再生成は行われない。これにより、可換記録媒体２０から別の可換記録媒体に複写された場合でも、別の可換記録媒体の媒体ＩＤにより、許諾コードＬ２が生成されることがないので、別の可換記録媒体に複写されたコンテンツが利用されることはない。

【００７３】図６は、許諾コードＬ２が可換記録媒体２０に記録された後に行われるコンテンツの復号過程を説明する為の説明図である。この復号過程では、まず、可換記録媒体２０から媒体ＩＤと許諾コードＬ２とを読み出す。次に、この媒体ＩＤと許諾コードＬ２とから、暗号鍵生成アルゴリズムを備えたハードウェア又はソフトウェア２７を用いて、暗号鍵Ｋを生成する。次に、暗号鍵Ｋから、復号アルゴリズムを備えたハードウェア又はソフトウェア２８を用いて、コンテンツＣをコンテンツＰに復号する。これにより、コンテンツＣの利用が可能となり、また、許諾コードの変更後は、ドライブＩＤが異なる可換記録媒体用ドライブ装置であっても、コンテンツＣを利用することが可能となる。

【００７４】尚、図５に示した許諾コードの変更を行わずに、実施の形態１の図２に示したように、直接、暗号化されたコンテンツＣをコンテンツＰに復号してもよい。但し、この場合は、製品構成ＩＤに替えて、可換記録媒体用ドライブ装置２４から得られたドライブＩＤを使用する。これにより、ドライブＩＤが異なる可換記録媒体用ドライブ装置では、コンテンツＣを利用することができなくなる。

【００７５】本発明に係る再生許可方法の実施の形態２に使用する可換記録媒体の製造工程は、前述した本発明に係る再生許可方法の実施の形態１に使用する可換記録媒体の製造程（図３）と略同様であるので、説明を省略する。但し、実施の形態２に使用する可換記録媒体の製造工程では、図３における製品構成ＩＤに替わって、可換記録媒体用ドライブ装置メーカによって決められたドライブＩＤであり、ＩＤ記録機８５により記録されるＩＤは、媒体ＩＤのみである。

【００７６】実施の形態３．図７は、第３，６，８発明に係る再生許可方法及び第１２発明に係る記録方法の実施の形態３に使用する可換記録媒体３０に記録されたコンテンツが、初めて利用される前に行われる許諾コードの変更方法及びコンテンツの再暗号化を説明する為の説明図である。書き換えが可能な可換記録媒体３０に記録する情報の生成方法は、前述した実施の形態２において、図４を参照しながら説明した生成方法と同様であるので、説明を省略する。　コンテンツ使用者が可換記録媒体３０に記録されたコンテンツＣを利用するとき、可換記録媒体用ドライブ装置３１は、まず、可換記録媒体３０に記録されているコンテンツ利用情報を参照し、コンテンツが既に利用されているか否かを検査する。コンテンツが利用されていないときは、ドライブＩＤに依存する許諾コードＬ１を、媒体ＩＤに依存する許諾コードＬ２（第２の暗号化情報）に変更し、また、コンテンツＣ（第１の暗号化記録情報）を別の暗号アルゴリズムにより、コンテンツＣ２（第２の暗号化記録情報）に再暗号化する。

【００７７】許諾コードＬ１から許諾コードＬ２への変更及びコンテンツＣからコンテンツＣ２への再暗号化は、以下のように行われる。可換記録媒体用ドライブ装置３１から得られたドライブＩＤと、可換記録媒体３０から読み出された許諾コードＬ１とから、暗号鍵生成アルゴリズムを備えたハードウェア又はソフトウェア３２を用いて、暗号鍵Ｋを一時的に生成する。これにより、ドライブＩＤが異なる可換記録媒体用ドライブ装置では、暗号鍵Ｋを生成することができず、許諾コードの変更及びコンテンツの再暗号化を行うことはできない。

【００７８】一方、許諾コード生成アルゴリズムを備えたハードウェア又はソフトウェア３４を用いて、可換記録媒体３０から読み出した媒体ＩＤと、暗号鍵Ｋではない別のコンテンツＰ用の暗号鍵Ｋ２（第２の暗号鍵）とから、許諾コードＬ２（第２の暗号化情報）を生成し、可換記録媒体３０の書き換えが可能な領域に記録する。次に、順次、可換記録媒体３０からコンテンツＣを読み出し、復号アルゴリズムを備えたハードウェア又はソフトウェア３３を用いて暗号鍵Ｋにより、コンテンツＰへ復号し、復号したコンテンツＰを、暗号アルゴリズムを備えたハードウェア又はソフトウェア３５を用いて暗号鍵Ｋ２により、コンテンツＣ２へ再暗号化し、可換記録媒体３０の書き換えが可能な領域に記録する。

【００７９】許諾コードＬ２及び再暗号化したコンテンツＣ２を可換記録媒体３０に記録した後、可換記録媒体３０上のコンテンツ利用情報を「コンテンツは既に利用された」の意味に変更する。これにより、以後、コンテンツ利用情報を参照することによって、「コンテンツは既に利用された」と判断され、許諾コードＬ２の再生成は行われない。

【００８０】これにより、可換記録媒体３０から別の可換記録媒体に複写された場合でも、別の可換記録媒体の媒体ＩＤにより、許諾コードＬ２が生成されることがなく、別の可換記録媒体に複写されたコンテンツが利用されることはない。また、許諾コードの変更及びコンテン

ツの再暗号化後は、ドライブＩＤが異なる可換記録媒体用ドライブ装置でも、可換記録媒体３０を利用でき、コンテンツを読み出すことができる。

【００８１】許諾コードＬ２が可換記録媒体３０に記録された後に行われるコンテンツの復号過程は、前述した実施の形態２において、図６を参照しながら説明した復号過程と同様であるので、説明を省略する。但し、実施の形態３では、図６における暗号鍵Ｋ及びコンテンツＣは、それぞれ暗号鍵Ｋ２及びコンテンツＣ２である。可換記録媒体３０の製造工程は、前述した実施の形態１の可換記録媒体の製造工程（図３）と略同様であるので、説明を省略する。但し、可換記録媒体３０の製造工程では、図３における製品構成ＩＤに替わって、可換記録媒体用ドライブ装置メーカによって決められたドライブＩＤであり、ＩＤ記録機８５により記録されるＩＤは、媒体ＩＤのみである。

【００８２】実施の形態４．図８は、第３，７，８発明に係る再生許可方法及び第１３発明に係る記録方法の実施の形態４を説明する為の説明図であり、書き換えが可能な可換記録媒体に記録する情報の生成方法を説明する為の説明図である。この生成方法は、可換記録媒体用ドライブ装置メーカ４１によって決められ、可換記録媒体用ドライブ装置に記録されているドライブＩＤから、暗号鍵生成アルゴリズムを備えたハードウェア又はソフトウェア４２を用いて、コンテンツＰ用の暗号鍵Ｋを生成する。

【００８３】次に、コンテンツＰ用の暗号鍵Ｋから、暗号アルゴリズムを備えたハードウェア又はソフトウェア４３を用いて、コンテンツＰを暗号化してコンテンツＣを生成し、可換記録媒体４０の書き換えが可能な領域に記録する。可換記録媒体毎の媒体ＩＤは、可換記録媒体２０の書き換えが不可能な領域に記録する。

【００８４】従来の再生許可方法（図１６）では、媒体ＩＤに依存した許諾コードＬ０を生成していたが、媒体ＩＤ毎に許諾コードＬ０を生成しなければならないので、製造設備が複雑になり、製造コストの上昇を招いていた。一方、図８に示した再生許可方法では、ドライブＩＤ毎にコンテンツＣが共通のデータとなり、従来の再生許可方法（図１６）より製造設備が簡単になり、製造コストを低く押さえることが可能となる。

【００８５】図９は、可換記録媒体４０に記録されたコンテンツが初めて利用される前に行われるコンテンツの再暗号化を説明する為の説明図である。コンテンツ使用者が可換記録媒体４０に記録されたコンテンツＣを利用するとき、可換記録媒体用ドライブ装置４４は、まず、可換記録媒体４０に記録されているコンテンツ利用情報を参照し、コンテンツが既に利用されているか否かを検査する。コンテンツが利用されていないときは、コンテンツＣを別の暗号アルゴリズムにより、コンテンツＣ２に再暗号化する。

【００８６】コンテンツＣからコンテンツＣ２（第２の暗号化記録情報）への再暗号化は、以下のように行われる。可換記録媒体用ドライブ装置４４から得られたドライブＩＤから、暗号鍵生成アルゴリズムを備えたハードウェア又はソフトウェア４２を用いて、暗号鍵Ｋを一時的に生成する。これにより、ドライブＩＤが異なる可換記録媒体用ドライブ装置では、暗号鍵Ｋを生成することができず、許諾コードの変更及びコンテンツの再暗号化を行うことはできない。

【００８７】一方、暗号鍵生成アルゴリズムを備えたハードウェア又はソフトウェア４７を用いて、可換記録媒体４０から読み出した媒体ＩＤから、暗号鍵Ｋではない別のコンテンツＰ用の暗号鍵Ｋ２（第２の暗号鍵）を生成する。次に、順次、可換記録媒体４０からコンテンツＣを読み出し、復号アルゴリズムを備えたハードウェア又はソフトウェア４６を用いて暗号鍵Ｋにより、コンテンツＰへ復号し、復号したコンテンツＰを、暗号アルゴリズムを備えたハードウェア又はソフトウェア４８を用いて暗号鍵Ｋ２により、コンテンツＣ２へ再暗号化し、可換記録媒体４０の書き換えが可能な領域に記録する。

【００８８】再暗号化したコンテンツＣ２を可換記録媒体４０に記録した後、可換記録媒体４０上のコンテンツ利用情報を「コンテンツは既に利用された」の意味に変更する。これにより、以後、コンテンツ利用情報を参照することによって、「コンテンツは既に利用された」と判断され、コンテンツＣからコンテンツＣ２への再暗号化は行われない。これにより、可換記録媒体４０から別の可換記録媒体に複写された場合でも、別の可換記録媒体の媒体ＩＤにより、暗号鍵Ｋ２が生成されることがなく、別の可換記録媒体に複写されたコンテンツが利用されることはない。

【００８９】図１０は、再暗号化されたコンテンツＣ２が可換記録媒体４０に記録された後に行われるコンテンツの復号過程を説明する為の説明図である。この復号過程では、まず、可換記録媒体４０から媒体ＩＤを読み出す。次に、この媒体ＩＤから、暗号鍵生成アルゴリズムを備えたハードウェア又はソフトウェア４９を用いて、暗号鍵Ｋ２を生成する。次に、暗号鍵Ｋ２から、復号アルゴリズムを備えたハードウェア又はソフトウェア５０を用いて、コンテンツＣ２をコンテンツＰに復号する。これにより、コンテンツＣの利用が可能となり、また、許諾コードの変更及びコンテンツの再暗号化後は、ドライブＩＤが異なる可換記録媒体用ドライブ装置であっても、コンテンツＣを利用することが可能となる。

【００９０】本発明に係る再生許可方法の実施の形態４に使用する可換記録媒体の製造工程は、前述した本発明に係る再生許可方法の実施の形態１に使用する可換記録媒体の製造程（図３）と略同様であるので、説明を省略する。但し、実施の形態４に使用する可換記録媒体の製造工程では、図３における製品構成ＩＤに替わって、可

換記録媒体用ドライブ装置メーカによって決められたドライブＩＤであり、ＩＤ記録機８５により記録されるＩＤは、媒体ＩＤのみである。また、複写機８２により複写される情報は、暗号化されたコンテンツ群のみである。

【００９１】実施の形態５．図１１は、第１７発明に係る記録媒体の実施の形態の構成例を説明する為の説明図である。この実施の形態では、読み出した、前記記録情報に固有の情報を用いて第１の暗号化情報を第１の暗号鍵に復号化するステップＳＴ１０と、復号化した第１の暗号鍵を用いて第１の暗号化記録情報を前記記録情報に復号化するステップＳＴ１１とを含むコンピュータプログラムＰＲ１を記録してあるＣＤ－ＲＯＭ（ＣＤ１）が、ディスクドライブＤＤに装填され、その内容はパーソナルコンピュータＰＣに読み込まれる。

【００９２】コンピュータプログラムＰＲ１が読み込まれた後は、ＣＤ－ＲＯＭ（ＣＤ１）はディスクドライブＤＤから取り出され、ディスクドライブＤＤには、例えば、可換記録媒体１０（図１）が装填され、その内容がパーソナルコンピュータＰＣに読み込まれる。パーソナルコンピュータＰＣのその他の動作は、実施の形態１で説明したコンテンツＣの利用方法と同様であるので、説明を省略する。

【００９３】実施の形態６．図１２は、第１８発明に係る記録媒体の実施の形態の構成例を説明する為の説明図である。この実施の形態では、ディスクドライブＤＤ（適用記録媒体用ドライブ装置）に記録されているディスクドライブＤＤに固有の情報を用いて第１の暗号化情報を第１の暗号鍵に復号化するステップＳＴ２０と、復号化した第１の暗号鍵を用いて第１の暗号化記録情報を前記記録情報に復号化するステップＳＴ２１とを含むコンピュータプログラムＰＲ２を記録してあるＣＤ－ＲＯＭ（ＣＤ２）が、ディスクドライブＤＤに装填され、その内容はパーソナルコンピュータＰＣに読み込まれる。

【００９４】コンピュータプログラムＰＲ２が読み込まれた後は、ＣＤ－ＲＯＭ（ＣＤ２）はディスクドライブＤＤから取り出され、ディスクドライブＤＤには、例えば、可換記録媒体２０（図４）が装填され、その内容がパーソナルコンピュータＰＣに読み込まれる。パーソナルコンピュータＰＣのその他の動作は、実施の形態２で説明したコンテンツＣの利用方法と同様であるので、説明を省略する。

【００９５】実施の形態７．図１３は、第１９発明に係る記録媒体の実施の形態の構成例を説明する為の説明図である。この実施の形態では、最初の再生に先立って、ディスクドライブＤＤ（前記適用記録媒体用ドライブ装置）に記録されているディスクドライブＤＤに固有の情報を用いて第１の暗号化情報を第１の暗号鍵に復号化するステップＳＴ３０と、復号化した第１の暗号鍵を、所定の第２の情報を用いて第２の暗号化情報に暗号化するステップＳＴ３１と、第２の暗号化情報を第１の暗号化情報に替えて前記適用記録媒体上の書き換え可能な領域に記録するステップＳＴ３２と、再生時に、第２の情報を用いて第２の暗号化情報を第１の暗号鍵に復号化するステップＳＴ３３と、復号化した第１の暗号鍵を用いて第１の暗号化記録情報を前記記録情報に復号化するステップＳＴ３４とを含むコンピュータプログラムＰＲ３を記録してあるＣＤ－ＲＯＭ（ＣＤ３）が、ディスクドライブＤＤに装填され、その内容はパーソナルコンピュータＰＣに読み込まれる。

【００９６】コンピュータプログラムＰＲ３が読み込まれた後は、ＣＤ－ＲＯＭ（ＣＤ３）はディスクドライブＤＤから取り出され、ディスクドライブＤＤには、例えば、可換記録媒体２０（図４）が装填され、その内容がパーソナルコンピュータＰＣに読み込まれる。パーソナルコンピュータＰＣのその他の動作は、実施の形態２で説明したコンテンツＣの利用方法と同様であるので、説明を省略する。

【００９７】実施の形態８．図１４は、第２０発明に係る記録媒体の実施の形態の構成例を説明する為の説明図である。この実施の形態では、最初の再生に先立って、ディスクドライブＤＤ（前記適用記録媒体用ドライブ装置）に記録されているディスクドライブＤＤに固有の情報を用いて第１の暗号化情報を第１の暗号鍵に復号化するステップＳＴ４０と、復号化した第１の暗号鍵を用いて第１の暗号化記録情報を前記記録情報に復号化するステップＳＴ４１と、復号化した前記記録情報を、第２の暗号鍵を用いて第２の暗号化記録情報に暗号化するステップＳＴ４２と、所定の第２の情報を用いて第２の暗号鍵を第３の暗号化情報に暗号化するステップＳＴ４３と、第３の暗号化情報を第１の暗号化情報に替えて、また、第２の暗号化記録情報を前記記録媒体上の書き換え可能な領域に記録するステップＳＴ４４と、再生時に、第２の情報を用いて第３の暗号化情報を第２の暗号鍵に復号化するステップＳＴ４５と、復号化した第２の暗号鍵を用いて第２の暗号化記録情報を前記記録情報に復号化するステップＳＴ４６とを含むコンピュータプログラムＰＲ４を記録してあるＣＤ－ＲＯＭ（ＣＤ４）が、ディスクドライブＤＤに装填され、その内容はパーソナルコンピュータＰＣに読み込まれる。

【００９８】コンピュータプログラムＰＲ４が読み込まれた後は、ＣＤ－ＲＯＭ（ＣＤ４）はディスクドライブＤＤから取り出され、ディスクドライブＤＤには、例えば、可換記録媒体３０（図７）が装填され、その内容がパーソナルコンピュータＰＣに読み込まれる。パーソナルコンピュータＰＣのその他の動作は、実施の形態３で説明したコンテンツＣの利用方法と同様であるので、説明を省略する。

【００９９】実施の形態９．図１５は、第２１発明に係る記録媒体の実施の形態の構成例を説明する為の説明図

である。この実施の形態では、最初の再生に先立って、ディスクドライブＤＤ（前記適用記録媒体用ドライブ装置）に記録されているディスクドライブＤＤに固有の情報を第１の暗号鍵に暗号化するステップＳＴ５０と、第１の暗号鍵を用いて第１の暗号化記録情報を前記記録情報に復号化するステップＳＴ５１と、所定の第２の情報を第２の暗号鍵に暗号化するステップＳＴ５２と、復号化した前記記録情報を、第２の暗号鍵を用いて第２の暗号化記録情報に暗号化するステップＳＴ５３と、第２の暗号化記録情報を前記記録媒体上の書き換え可能な領域に記録するステップＳＴ５４と、再生時に、第２の情報を第２の暗号鍵に暗号化するステップＳＴ５５と、第２の暗号鍵を用いて第２の暗号化記録情報を前記記録情報に復号化するステップＳＴ５６とを含むコンピュータプログラムＰＲ５を記録してあるＣＤ－ＲＯＭ（ＣＤ５）が、ディスクドライブＤＤに装填され、その内容はパーソナルコンピュータＰＣに読み込まれる。

【０１００】コンピュータプログラムＰＲ５が読み込まれた後は、ＣＤ－ＲＯＭ（ＣＤ５）はディスクドライブＤＤから取り出され、ディスクドライブＤＤには、例えば、可換記録媒体４０（図８）が装填され、その内容がパーソナルコンピュータＰＣに読み込まれる。パーソナルコンピュータＰＣのその他の動作は、実施の形態４で説明したコンテンツＣの利用方法と同様であるので、説明を省略する。

【０１０１】尚、図５では、ドライブＩＤに依存した許諾コードＬ１から、媒体ＩＤに依存した許諾コードＬ２へ変更する方法を示したが、媒体ＩＤの替わりに、コンテンツ使用者毎に固有の情報に依存した許諾コードに変更してもよい。コンテンツ使用者毎に固有の情報とは、具体的には、コンピュータのＯＳが管理しているユーザＩＤ又はＩＣカードに記録されているユーザＩＤ等である。その結果、可換記録媒体２０に記録されたコンテンツは、特定のコンピュータ又は特定のユーザによる以外に利用することができなくなる。

【０１０２】また、媒体ＩＤに依存した許諾コード、又はユーザ毎に固有の情報に依存した許諾コードの他に、可換記録媒体用ドライブ装置を制御するコンピュータに固有の情報に依存した許諾コードに変更してもよい。コンピュータに固有の情報とは、具体的には、コンピュータのＢＩＯＳ（Basic Input Output System ）が有するマシンＩＤ等である。その結果、可換記録媒体に記録されたコンテンツは、特定のコンピュータによる以外に利用することができなくなる。このように、許諾コードをどのような情報に依存させるかによって、様々なコンテンツ使用範囲を設定することができるが、これらは、コンテンツの著作権所有者に委ねられる。また、実施の形態５～９に記述した記録媒体は、ＣＤ－ＲＯＭに限らずハードディスク又は可換記録媒体等であっても良いことは言うまでもない。

【０１０３】

【発明の効果】第１発明に係る再生許可方法によれば、記録情報が同じである記録媒体は、一括して製造、検査を行うことができ、製造コストの上昇を招くことなく、記録媒体に記録された情報の著作権を保護することができる。

【０１０４】第２発明に係る再生許可方法によれば、別の記録媒体に複写した場合、記録情報に固有の情報は複写されないので、第１の暗号鍵が復号化できず、記録情報を復号化できない。従って、記録媒体に記録されている記録情報の著作権を保護することができる。また、記録情報が同じである記録媒体は、一括して製造、検査を行うことができるので、製造コストの上昇を招くことがない。

【０１０５】第３発明に係る再生許可方法によれば、ドライブ装置に固有の情報が異なるドライブ装置による再生は行えず、記録媒体に記録されている記録情報の著作権を保護することができる。また、同じドライブ装置に固有の情報による暗号化情報を記録される記録媒体は、一括して製造、検査を行うことができるので、製造コストの上昇を招くことがない。

【０１０６】第４発明に係る再生許可方法によれば、ドライブ装置に固有の情報が異なるドライブ装置による再生は行えず、記録媒体に記録されている記録情報の著作権を保護することができる。また、同じドライブ装置に固有の情報による暗号化情報を記録される記録媒体は、一括して製造、検査を行うことができるので、製造コストの上昇を招くことがない。

【０１０７】第５発明に係る再生許可方法によれば、最初の再生に先立つ暗号化情報の変更を、ドライブ装置に固有の情報が異なるドライブ装置では行えず、また、暗号化情報の変更後は、別の記録媒体に複写した場合に、第２の情報がなければ、記録情報に復号化することができないので、記録媒体に記録されている記録情報の著作権を保護することができる。また、同じドライブ装置に固有の情報による暗号化情報を記録される記録媒体は、一括して製造、検査を行うことができるので、製造コストの上昇を招くことがない。

【０１０８】第６発明に係る再生許可方法によれば、最初の再生に先立つ暗号化情報及び暗号化記録情報の変更を、ドライブ装置に固有の情報が異なるドライブ装置では行えず、また、暗号化情報及び暗号化記録情報の変更後は、別の記録媒体に複写した場合に、第２の情報がなければ、記録情報に復号化することができないので、記録媒体に記録されている記録情報の著作権を保護することができる。また、同じドライブ装置に固有の情報による暗号化情報を記録される記録媒体は、一括して製造、検査を行うことができるので、製造コストの上昇を招くことがない。

【０１０９】第７発明に係る再生許可方法によれば、最

初の再生に先立つ暗号化記録情報の変更を、ドライブ装置に固有の情報が異なるドライブ装置では行えず、また、暗号化記録情報の変更後は、別の記録媒体に複写した場合に、第２の情報がなければ、記録情報に復号化することができないので、記録媒体に記録されている記録情報の著作権を保護することができる。また、同じドライブ装置に固有の情報による暗号鍵により暗号化された暗号化記録情報を記録される記録媒体は、一括して製造、検査を行うことができるので、製造コストの上昇を招くことがない。

【０１１０】第８発明に係る再生許可方法によれば、最初の再生に先立つ暗号化情報又は暗号化記録情報の変更後は、別の記録媒体に複写した場合に、記録媒体毎に固有の情報は複写されず、記録情報に復号化することができないので、記録媒体に記録されている記録情報の著作権を保護することができる。

【０１１１】第９発明に係る再生許可方法によれば、最初の再生に先立つ暗号化情報又は暗号化記録情報の変更後は、別の記録媒体に複写した場合に、ユーザが異なれば、記録情報に復号化することができないので、記録媒体に記録されている記録情報の著作権を保護することができる。

【０１１２】第１０発明に係る再生許可方法によれば、最初の再生に先立つ暗号化情報又は暗号化記録情報の変更後は、別の記録媒体に複写した場合に、ドライブ装置を制御するコンピュータが異なれば、記録情報に復号化することができないので、記録媒体に記録されている記録情報の著作権を保護することができる。

【０１１３】第１１発明に係る記録方法によれば、別の記録媒体に複写した場合、記録情報に固有の情報は複写されないので、第１の暗号鍵が復号化できず、記録情報を再生できない。従って、記録媒体に記録されている記録情報の著作権を保護することができる。また、記録情報が同じである記録媒体は、その他の内容構成も同一となり、一括して製造、検査を行うことができるので、製造コストの上昇を招くことがない。

【０１１４】第１２発明に係る記録方法によれば、ドライブ装置に固有の情報が異なるドライブ装置による再生は行えず、記録媒体に記録されている記録情報の著作権を保護することができる。また、ドライブ装置に固有の同じ情報による暗号化情報を記録される記録媒体は、その他の内容構成も略同一となり、一括して製造、検査を行うことができるので、製造コストの上昇を招くことがない。

【０１１５】第１３発明に係る記録方法によれば、最初の再生に先立つ暗号化記録情報の変更を、ドライブ装置に固有の情報が異なるドライブ装置では行えないので、記録媒体に記録されている記録情報の著作権を保護することができる。また、同じドライブ装置に固有の情報による暗号鍵により暗号化された暗号化記録情報を記録される記録媒体は、その他の内容構成も略同一となり、一括して製造、検査を行うことができるので、製造コストの上昇を招くことがない。

【０１１６】第１４，１５発明に係る記録媒体によれば、記録情報が同じであれば、一括して製造、検査を行うことができ、製造コストの上昇を招くことなく、記録された情報の著作権を保護することができる。

【０１１７】第１６発明に係る記録媒体によれば、ドライブ装置に固有の情報が異なるドライブ装置による再生は行えず、記録されている記録情報の著作権を保護することができる。また、同じドライブ装置に固有の情報による暗号化情報を記録される記録媒体は、一括して製造、検査を行うことができるので、製造コストの上昇を招くことがない。

【０１１８】第１７発明に係る記録媒体が記録しているプログラムにより制御されるコンピュータによれば、別の記録媒体に複写した場合、記録情報に固有の情報は複写されないので、第１の暗号鍵が復号化できず、記録情報を再生できない。従って、記録媒体に記録されている記録情報の著作権を保護することができる。

【０１１９】第１８発明に係る記録媒体が記録しているプログラムにより制御されるコンピュータによれば、ドライブ装置に固有の情報が異なるドライブ装置による再生は行えず、記録媒体に記録されている記録情報の著作権を保護することができる。

【０１２０】第１９発明に係る記録媒体が記録しているプログラムにより制御されるコンピュータによれば、最初の再生に先立つ暗号化情報の変更を、ドライブ装置に固有の情報が異なるドライブ装置では行えず、また、暗号化情報の変更後は、別の記録媒体に複写した場合に、第２の情報がなければ、記録情報に復号化することができないので、記録媒体に記録されている記録情報の著作権を保護することができる。

【０１２１】第２０発明に係る記録媒体が記録しているプログラムにより制御されるコンピュータによれば、最初の再生に先立つ暗号化情報及び暗号化記録情報の変更を、ドライブ装置に固有の情報が異なるドライブ装置では行えず、また、暗号化情報及び暗号化記録情報の変更後は、別の記録媒体に複写した場合に、第２の情報がなければ、記録情報に復号化することができないので、記録媒体に記録されている記録情報の著作権を保護することができる。

【０１２２】第２１発明に係る記録媒体が記録しているプログラムにより制御されるコンピュータによれば、最初の再生に先立つ暗号化記録情報の変更を、ドライブ装置に固有の情報が異なるドライブ装置では行えず、また、暗号化記録情報の変更後は、別の記録媒体に複写した場合に、第２の情報がなければ、記録情報に復号化することができないので、記録媒体に記録されている記録情報の著作権を保護することができる。

29

【図面の簡単な説明】

【図１】第１，２発明に係る再生許可方法、第１１発明に係る記録方法及び第１４，１５発明に係る記録媒体の実施の形態１を説明する為の説明図である。

【図２】可換記録媒体に記録されたコンテンツの利用方法を説明する為の説明図である。

【図３】可換記録媒体の製造工程を説明する為の説明図である。

【図４】第３～５，８～１０発明に係る再生許可方法、第１２発明に係る記録方法及び第１６発明に係る記録媒体の実施の形態２を説明する為の説明図である。

【図５】可換記録媒体に記録されたコンテンツが初めて利用される前に行われる許諾コードの変更方法を説明する為の説明図である。

【図６】許諾コードＬ２が可換記録媒体に記録された後に行われるコンテンツの復号過程を説明する為の説明図である。

【図７】許諾コードの変更方法及びコンテンツの再暗号化を説明する為の説明図である。

【図８】第３，７，８発明に係る再生許可方法及び第１３発明に係る記録方法の実施の形態４を説明する為の説明図である。

【図９】可換記録媒体に記録されたコンテンツが初めて利用される前に行われるコンテンツの再暗号化を説明する為の説明図である。

【図１０】再暗号化されたコンテンツが可換記録媒体に記録された後に行われるコンテンツの復号過程を説明する為の説明図である。

30

＊【図１１】第１７発明に係る記録媒体の実施の形態の構成を説明する為の説明図である。

【図１２】第１８発明に係る記録媒体の実施の形態の構成を説明する為の説明図である。

【図１３】第１９発明に係る記録媒体の実施の形態の構成を説明する為の説明図である。

【図１４】第２０発明に係る記録媒体の実施の形態の構成を説明する為の説明図である。

【図１５】第２１発明に係る記録媒体の実施の形態の構成を説明する為の説明図である。

【図１６】従来の再生許可方法の一例を説明する為の説明図である。

【図１７】従来の再生許可方法の一例を説明する為の説明図である。

【符号の説明】

１０，２０，３０，４０　記録媒体（適用記録媒体）

１１，２２，２６，３４　許諾コード生成アルゴルズムを備えたハードウェア又はソフトウェア

１２，２３，３５，４３，４８　暗号アルゴルズムを備えたハードウェア又はソフトウェア

１３，２５，２７，３２，４２，４７，４９　暗号鍵生成アルゴルズムを備えたハードウェア又はソフトウェア

１４，２８．３３，４６，５０　復号アルゴルズムを備えたハードウェア又はソフトウェア

ＣＤ１～ＣＤ５　ＣＤ－ＲＯＭ（記録媒体）

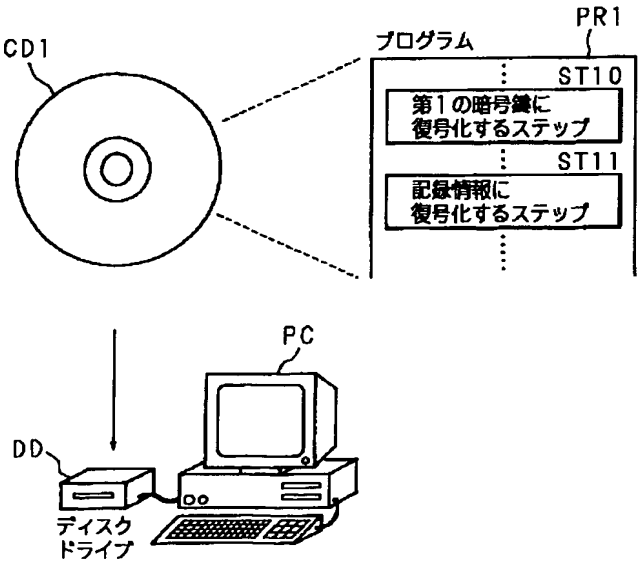
ＤＤ　ディスクドライブ

ＰＲ１～ＰＲ５　コンピュータプログラム

ＰＣ　パーソナルコンピュータ（コンピュータ）

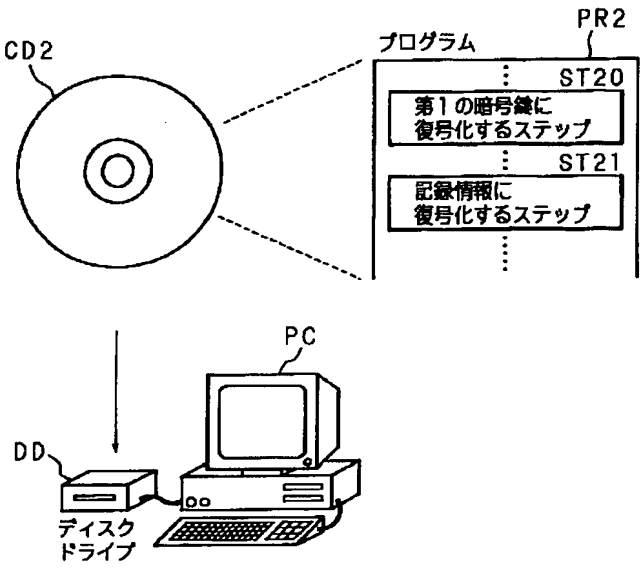
【図１１】

第１７発明に係る記録媒体の実施の形態の構成を説明する為の説明図



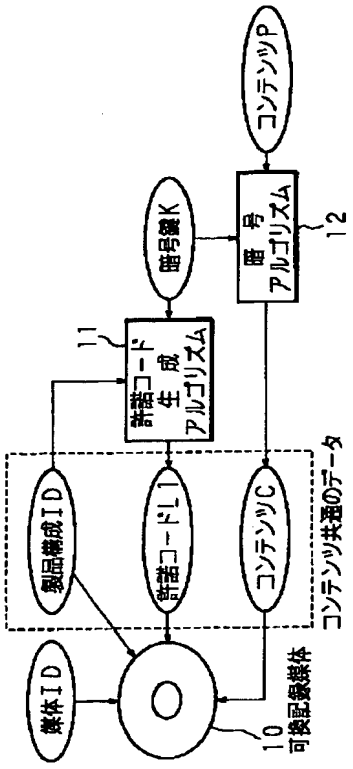
【図１２】

第１８発明に係る記録媒体の実施の形態の構成を説明する為の説明図



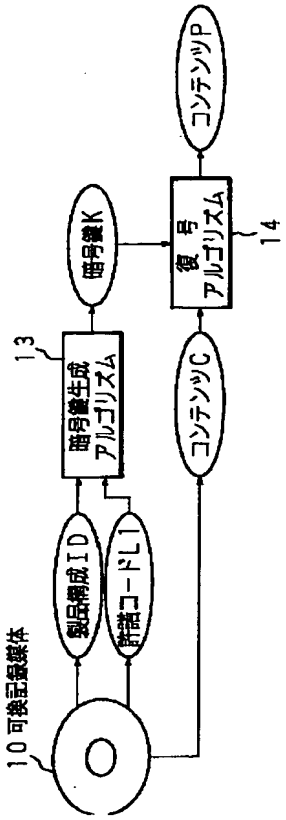
【図１】

第１，２発明に係る再生許可方法、第１１発明に係る記録方法及び第１４，１５発明に係る記録媒体の実施の形態１を説明するための説明図



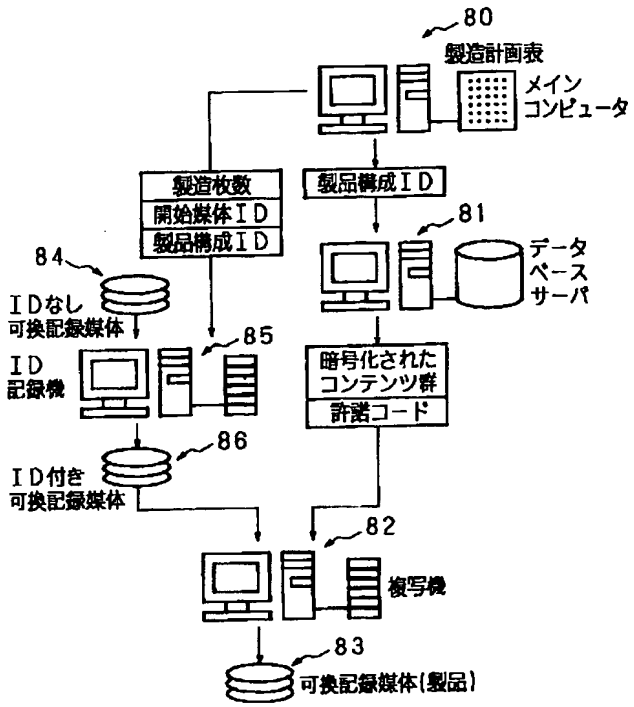
【図２】

可換記録媒体に記録されたコンテンツの利用方法を説明するための説明図



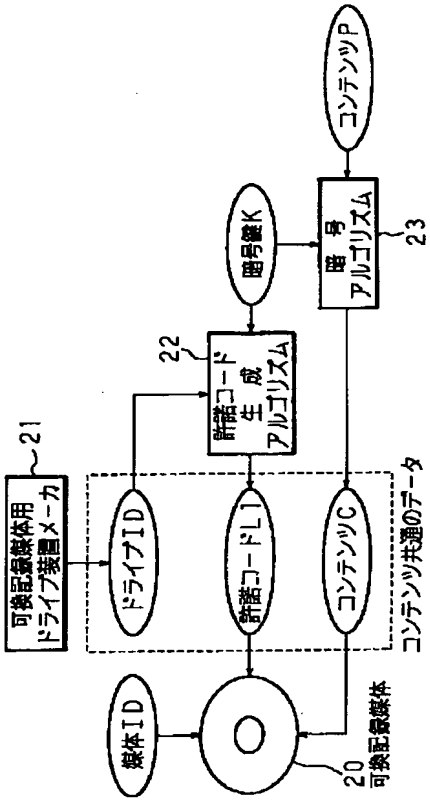
【図３】

可換記録媒体の製造工程を説明するための説明図



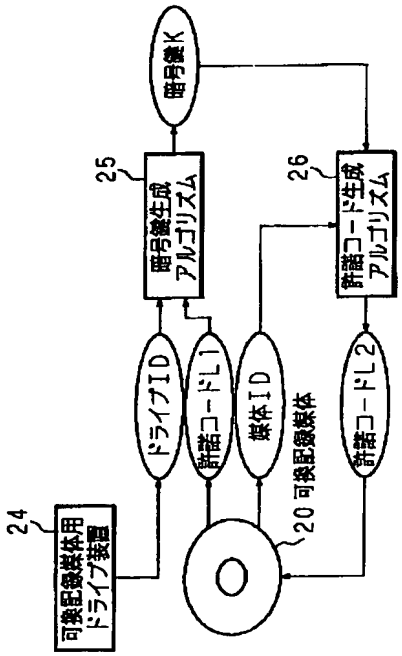
【図４】

第３～５，８～１０発明に係る再生許可方法、第１２発明に係る記録方法及び第１６発明に係る記録媒体の実施の形態２を説明するための説明図



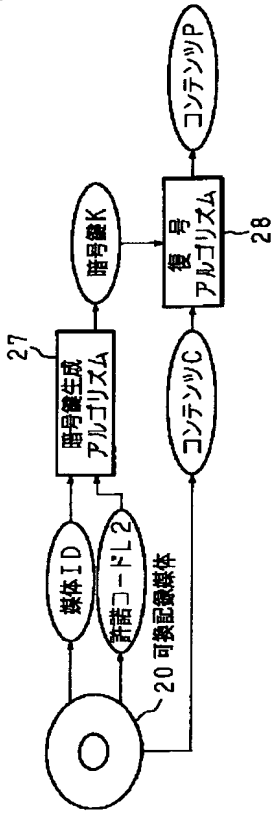
【図５】

可換記録媒体に記録されたコンテンツが初めて利用される前に行われる許諾コードの変更方法を説明するための説明図



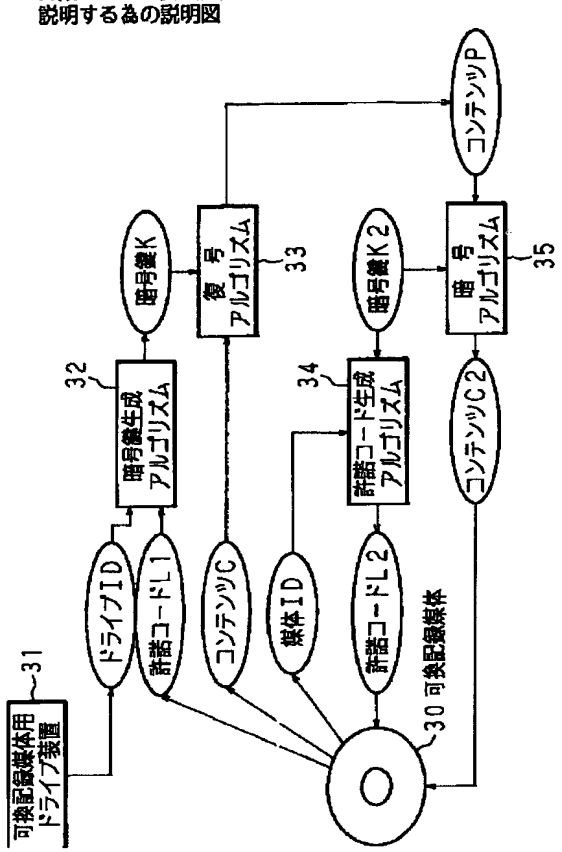
【図６】

許諾コードＬ２が可換記録媒体に記録された後に行われるコンテンツの復号過程を説明するための説明図



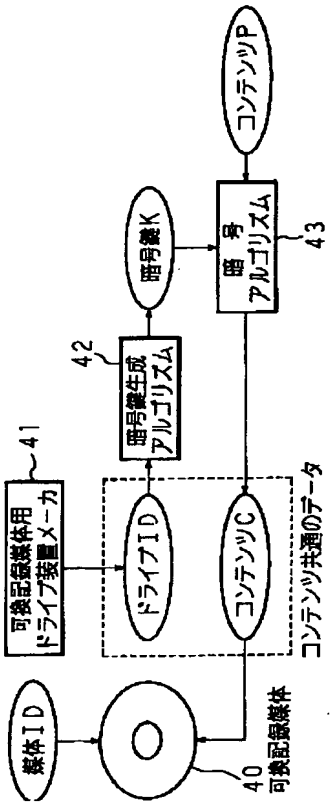
【図７】

許諾コードの変更方法及びコンテンツの再暗号化を説明するための説明図



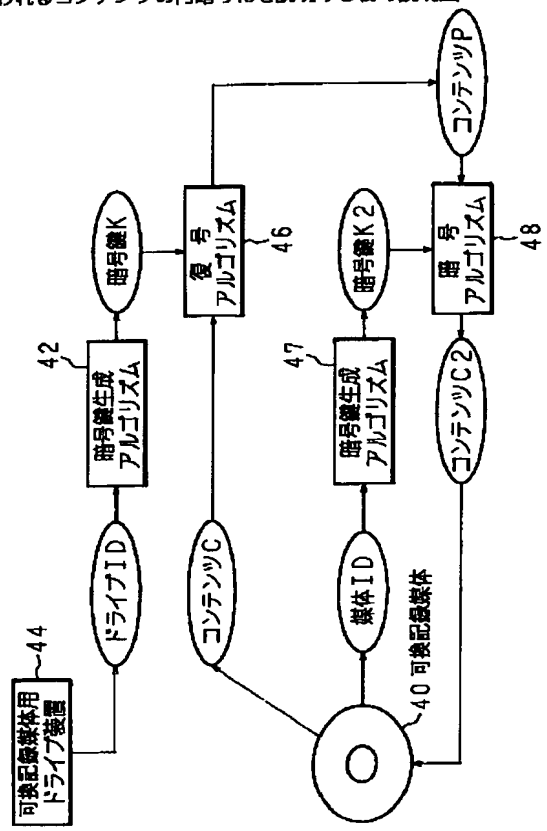
【図８】

第３，７，８発明に係る再生許可方法及び第１３発明に係る記録方法の実施の形態４を説明するための説明図



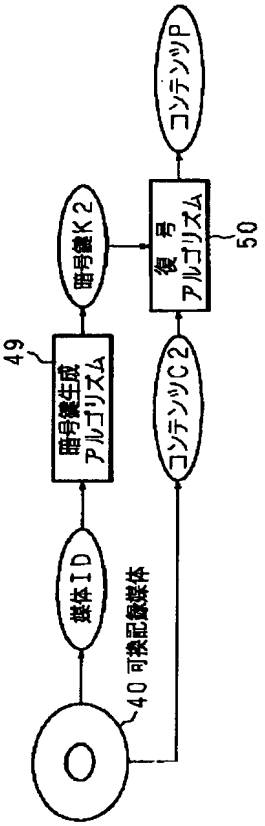
【図９】

可換記録媒体に記録されたコンテンツが初めて利用される前に行われるコンテンツの再暗号化を説明するための説明図



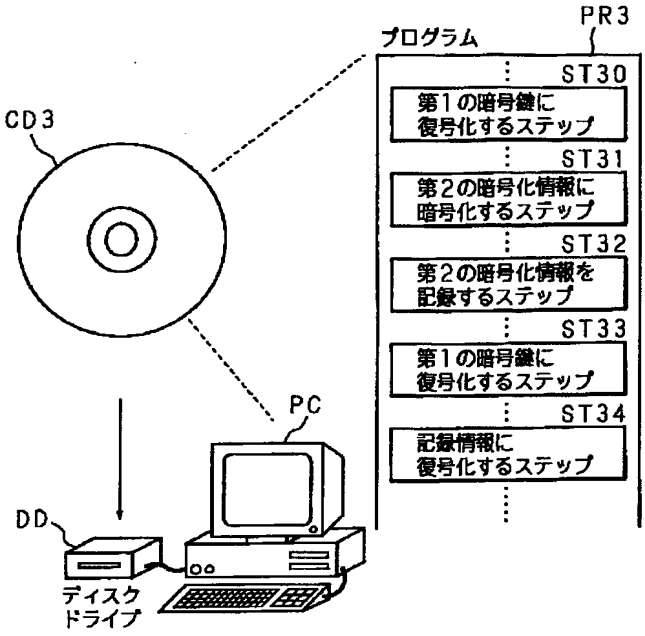
【図１０】

再暗号化されたコンテンツが可換記録媒体に記録された後に行われるコンテンツの復号過程を説明するための説明図



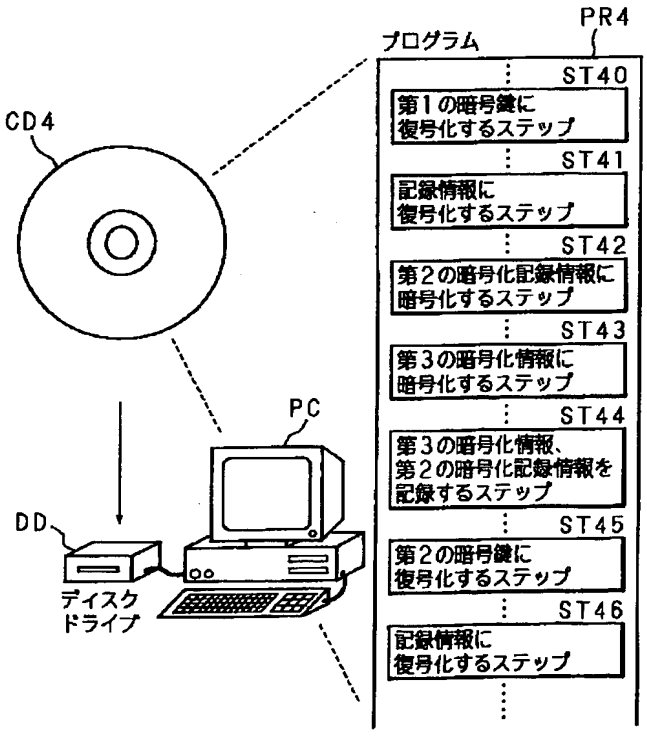
【図１３】

第１９発明に係る記録媒体の実施の形態の構成を説明するための説明図



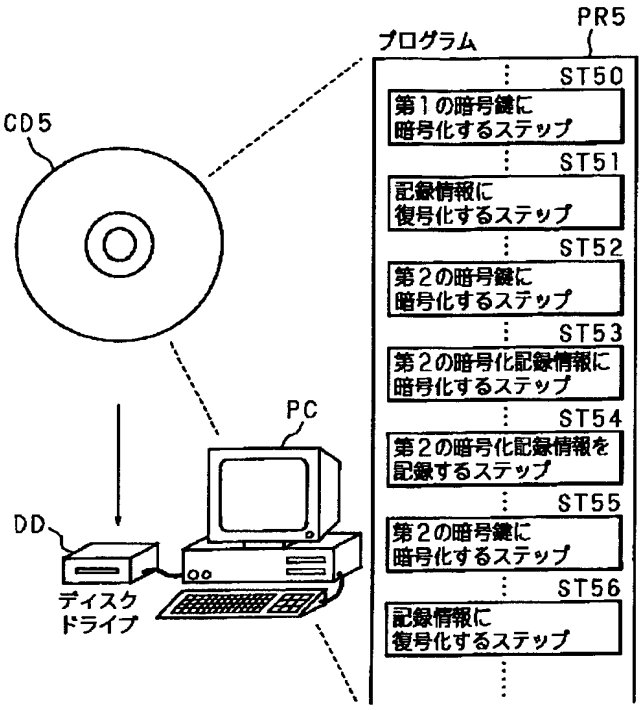
【図１４】

第２０発明に係る記録媒体の実施の形態の構成を説明するための説明図



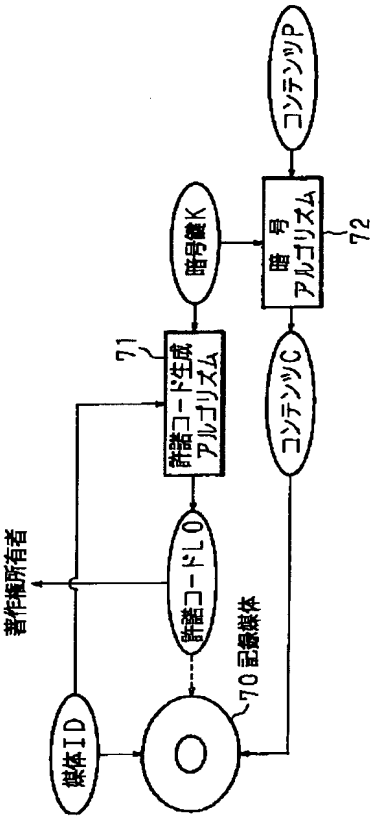
【図１５】

第２１発明に係る記録媒体の実施の形態の構成を説明するための説明図



【図１６】

従来の再生許可方法の一例を説明するための説明図



【図１７】

従来の再生許可方法の一例を説明するための説明図